CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE

FORMER NAME: CYBER SECURITY AND ARTIFICIAL INTELLIGENCE: EMERGING TRENDS

Editors:

Dr. Ausaf Ahmad Malik

Mr. Abhilash Aggarwal

Adv. Gyan Prakash Kesharwani

VidhiAagaz Inking Your Brain

Rai University EVO'V'NG THI'NK NG MINDS

CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE

Editorial Board:

1. **Dr. Ausaf Ahmad Malik** *[Principal and Professor, School of Law, Rai University, Ahmedabad]*
2. **Mr. Abhilash Aggarwal** *[Head of Department, School of Law, Rai University, Ahmedabad]*
3. **Adv. Gyan Prakash Kesharwani** *[Advocate & Chairperson, VidhiAagaz]*
4. **Mr. Dinesh Kumar Mishra** *[Assistant Professor. School of Law, Rai University, Ahmedabad]*
5. **Ms. Prachi Tripathi** *[Assistant Professor. School of Law, Rai University, Ahmedabad]*
6. **Adv. Aishwarya Gupta** *[Advocate & Editorial Head, CLRS, VidhiAagaz]*

Published by
Centre for Legal Research and Studies (CLRS), VIDHIAAGAZ

ISBN: *978-81-947620-5-8*

First Edition
2024

First Impression: 2024

CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE

Copyright © 2024, VIDHIAAGAZ, Maihar

ISBN: 978-81-947620-5-8

All rights reserved. No part of this publication may be copied, reproduced, adapted, abridged or translated, stored in a retrieval system, computer system photographic or other system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission in writing of the Publisher.

The views expressed are of the authors solely and do not reflect the views of the Editors & Publisher. Authors are solely responsible for the contents of the manuscript. Though all efforts are made to ensure the accuracy and correctness of the information published, the Editorial Team or the Publisher shall not be held responsible for any error caused Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

PREFACE

The rapid evolution of technology in recent years has brought significant advancements in the fields of cyber security and artificial intelligence, along with a host of unprecedented challenges. The increasing interdependence of these two domains has created a fertile ground for academic exploration, interdisciplinary research, and practical innovations. It is within this dynamic and evolving context that *Cyber Security Concerns and Use of Artificial Intelligence* has been conceived and brought to fruition.

This edited book is the result of the National Conference on Cyber Security and Artificial Intelligence, organized by School of Law, Rai University, Ahmedabad in collaboration with the Centre for Legal Research and Studies (CLRS), VidhiAagaz. The conference served as a platform for scholars, practitioners, and experts to exchange ideas, share insights, and engage in critical discussions on the latest trends, challenges, and opportunities in these vital areas. The papers presented at the conference have been meticulously selected, reviewed, and refined to ensure that this publication reflects the highest standards of academic rigor.

This book is a compilation of all papers, each offering unique perspectives on topics such as the ethical implications of artificial intelligence, emerging threats in cyber security, legal frameworks governing technology, and the intersection of law, policy, and innovation. The diversity of themes and the depth of research make this volume a valuable resource for students, researchers, policymakers, and professionals.

Bringing this book to life has been a collaborative journey. I extend my heartfelt gratitude to the contributors for their insightful research, the reviewers for their critical inputs, and the editorial team for their dedication and meticulous efforts. Special thanks are due to School of Law, Rai University for its support and to our distinguished dignitaries for their messages of encouragement and guidance.

We hope this book inspires further research, fosters innovation, and contributes meaningfully to the ongoing dialogue in these ever-evolving fields.

Aishwarya Gupta

Editorial Head

Centre for Legal Research and Studies, VidhiAagaz

MESSAGE FROM THE CHIEF PATRON

It is with immense pride and pleasure that I extend my heartfelt congratulations to all the contributors, editors, and organizers of this remarkable endeavor, which has culminated in the publication of the edited book *Cyber Security Concerns and Use of Artificial Intelligence*. This publication is a testament to the dedication and collaborative spirit of our academic community and beyond.

In an era driven by rapid technological advancements, addressing critical challenges in cyber security and artificial intelligence has never been more important. The insightful contributions within this volume not only reflect the depth of research undertaken by the authors but also their commitment to advancing knowledge in these dynamic and impactful fields.

At Rai University, we strive to foster an environment of innovation, academic excellence, and critical inquiry. This book is a shining example of these values in action. I commend the editors for their tireless efforts in compiling and curating the contributions, ensuring the highest standards of academic rigor.

I am confident that this book will serve as a valuable resource for scholars, practitioners, and students alike, inspiring further exploration and innovation in these vital areas of study.

My sincere gratitude extends to all the contributors and the editorial team for their hard work and dedication. May this publication pave the way for more such fruitful endeavors in the future.

Prof. Anil Tomar

Provost, Rai University, Ahmedabad

MESSAGE FROM THE PRINCIPAL

It gives me immense joy to witness the successful culmination of the National Conference on Cyber Security and Artificial Intelligence into this edited book, *Cyber Security Concerns and Use of Artificial Intelligence*. This publication is a milestone achievement for Rai University, reflecting our unwavering commitment to fostering cutting-edge research and innovation.

The themes explored in this book are of critical importance in today's rapidly evolving digital landscape. The insights and perspectives shared by scholars and practitioners in this volume offer a fresh outlook on the challenges and opportunities in these dynamic fields.

I congratulate the editorial team for their diligence and the contributors for their outstanding research. I am confident that this book will serve as an excellent resource for students, academics, and professionals, furthering their understanding of these pertinent topics.

My heartfelt appreciation goes to all who made this endeavor a reality. I look forward to seeing Rai University continue its journey of academic excellence and thought leadership.

Dr. Ausaf Ahmad Malik

Principal

School of Law, Rai University

MESSAGE FROM THE HEAD OF THE DEPARTMENT

It is an honor to pen this message for the edited book, *Cyber Security Concerns and Use of Artificial Intelligence*, which is the result of an engaging and enlightening academic exercise hosted by Rai University. The collaborative efforts of the authors, editors, and organizers have brought to life a publication that addresses some of the most critical and timely issues of our age.

At the School of Law, Rai University, we are deeply committed to encouraging interdisciplinary research and fostering an environment where innovative ideas flourish. This book is a perfect example of such an initiative, bridging legal, technological, and ethical perspectives in the domains of cyber security and artificial intelligence.

I extend my heartfelt congratulations to the editors for their meticulous efforts and to the contributors for their high-quality research. This book will undoubtedly contribute to the body of knowledge in these crucial areas and serve as an inspiration for future academic endeavors.

Mr. Abhilash Aggarwal

Head of Department

School of Law, Rai University

MESSAGE FROM THE CHAIRPERSON

It gives me immense pride to extend my warmest congratulations on the successful publication of the edited book *Cyber Security Concerns and Use of Artificial Intelligence*. This book is a significant achievement, reflecting the hard work, dedication, and academic excellence of everyone involved in this endeavor.

In an era defined by rapid digital transformation, the intersection of cyber security and artificial intelligence presents both unparalleled opportunities and complex challenges. This edited volume serves as an important contribution to these critical areas, offering valuable insights and diverse perspectives that will benefit students, researchers, and practitioners alike.

As the Chairperson of the Centre for Legal Research and Studies (CLRS), I take great satisfaction in seeing such collaborative efforts come to fruition. This book not only underscores the importance of interdisciplinary research but also highlights VidhiAagaz' and Rai University's commitment to fostering a vibrant academic culture.

I extend my sincere gratitude to the editors for their relentless efforts in compiling and refining these contributions, and to the authors for their thought-provoking research. I am confident that this publication will serve as a lasting resource, inspiring continued dialogue and innovation in these essential fields.

Adv. Gyan Prakash Kesharwani

Chairperson

Centre for Legal Research and Studies (CLRS), VidhiAagaz

MESSAGE FROM THE EDITORIAL HEAD

It is with great joy and a deep sense of accomplishment that I present this edited book, *Cyber Security Concerns and Use of Artificial Intelligence*. This publication represents the culmination of rigorous research, insightful discussions, and the collaborative spirit of contributors and editors alike.

In today's rapidly evolving digital era, the convergence of cyber security and artificial intelligence poses both opportunities and challenges. This book captures the essence of these dynamics through a collection of well-researched papers that delve into critical issues, explore innovative solutions, and provide a multidisciplinary perspective on the topic.

As the Editorial Head of the Centre for Legal Research and Studies (CLRS), it has been a privilege to work alongside a team of dedicated professionals and scholars who have put their heart and soul into making this publication a reality. My deepest appreciation goes out to the authors for their valuable contributions, the editors for their meticulous attention to detail, and the organizers for their unwavering support throughout this journey.

I am confident that this book will serve as an important resource for students, academics, and professionals seeking to explore the fascinating and complex realms of cyber security and artificial intelligence. It is my hope that this work inspires further research and innovation in these crucial fields.

Aishwarya Gupta

Editorial Head

Centre for Legal Research and Studies (CLRS)

EDITORIAL BOARD

Dr. Ausaf Ahmad Malik

Principal and Professor, School of Law, Rai University, Ahmedabad

Dr. Ausaf Ahmad Malik is a seasoned academician with over 15 years of experience in teaching and administration across various universities in India. He holds a doctorate from the prestigious Jamia Millia Islamia, New Delhi, and an LL.M from Aligarh Muslim University, Aligarh. His academic contributions include the publication of over 16 research papers in national and international journals, authorship of one book, and editorial work on two books. Dr. Malik has also actively participated in numerous international and national seminars, conferences, and moot court competitions, often serving as a guest or chair at events hosted by eminent universities and colleges in India.

Mr. Abhilash Aggarwal

Head of Department, School of Law, Rai University, Ahmedabad

Mr. Abhilash Aggarwal is an accomplished legal scholar with expertise in Constitutional and Administrative Law, holding a Gold Medal from the National University of Study and Research in Law, Ranchi. He is a graduate of Jamia Millia Islamia, New Delhi, and has been a full-time research scholar at the Central University of Haryana, Mahendragarh. Mr. Aggarwal has previously served as an Assistant Professor at private institutes in Indore and New Delhi and as a guest faculty member at Jamia Millia Islamia. His research acumen extends to Family Law, Election Law, Criminal Law, International Law, and Human Rights, with several publications and accolades at national and international forums. Since 2019, his journey in legal academia and research has been marked by a commitment to excellence and impactful contributions.

Mr. Gyan Prakash Kesharwani

Advocate [LL.M. (IP Laws), B.A.LL.B.], Chairperson at VidhiAagaz

Mr. Gyan Prakash Kesharwani is a legal professional with expertise in Motor Vehicle Act, Consumer Protection, Labour, and Intellectual Property Law matters. He holds an LL.M. in IP Laws from National Law University Jodhpur and has received multiple accolades in conferences and moot court competitions. As the founder of VidhiAagaz, an academic publication house with a global presence, Mr. Kesharwani has overseen publications indexed in HeinOnline and Manupatra, with contributors from over 50 countries. He has edited more than 24 books and journals and frequently shares his expertise as a guest speaker at various institutions.

Mr. Dinesh Kumar Mishra

Assistant Professor, School of Law, Rai University, Ahmedabad

Mr. Dinesh Kumar Mishra is a distinguished academic and researcher with expertise in Constitutional and Administrative Law. He holds an LL.M with distinction from Gujarat National Law University (GNLU) Silvassa and is a gold medalist in his BA.LLB from Kalinga University, Raipur. Having qualified the UGC NET, Mr. Mishra has demonstrated academic excellence and a strong commitment to research. His scholarly work encompasses topics such as women's rights, press freedom, and the impact of blockchain technology on governance. He has presented his research at prominent national and international conferences and actively contributes to the discourse on constitutional law and policy. His dedication to advancing legal scholarship positions him as a leading figure in legal academia.

Ms. Prachi Tripathi

Assistant Professor, School of Law, Rai University, Ahmedabad

Ms. Prachi Tripathi specializes in Corporate and Business Laws, holding a post-graduate degree from Himachal Pradesh National Law University, Shimla. Her expertise includes cyber laws, competition laws, mergers and acquisitions, and taxation. Ms. Tripathi has played an active role in organizing national conferences and moot court competitions, often serving as a judge for various national events. Her passion for research and academic contributions underscores her dedication to advancing the field of law. Her commitment to exploring new areas of legal scholarship and fostering legal education highlights her vital role in shaping the future of corporate law and policy.

Ms. Aishwarya Gupta

Advocate [B.A.LL.B.], Editorial Head at Centre for Legal Research & Studies, VidhiAagaz

Ms. Aishwarya Gupta is an Advocate practicing at the High Court of Madhya Pradesh, Indore Bench, with a specialization in Tax and Family Laws. She holds a B.A.LL.B. and actively contributes to legal research and academic publications as the Publishing Editor at VidhiAagaz. She has participated in several national and international conferences, showcasing her commitment to legal scholarship. Ms. Gupta’s combined experience in practice and publishing underscores her dedication to advancing legal education and research.

Her keen eye for detail, combined with her dedication to maintaining high standards of academic rigor, has ensured the quality and coherence of this edited book. Her work reflects her commitment to advancing legal scholarship and creating platforms for meaningful discourse.

TABLE OF CONTENTS

1. Legal Challenges in Cross-Border Data Transfers amid Financial Cyber Crimes……..01

Nandini Braj Singh & Disha Singhal [Student at Symbiosis Law School, NOIDA, India]

2. Cybersecurity Concerns and Use of Artificial Intelligence: Two Major Forces behind the Creation of Criminogenic Society Globally……..……..15

Maitri Shail Patel [Ph.D. Student at GLS University, Ahmedabad, India]

3. Empowering Elderly Individuals: The Role of Digital Media in Cybercrime…….22

Naina Chudasama [Student, UWSL , Karnavati University, India]

4. Cross-Border Cybercrime in the Metaverse: Navigating Jurisdictional Challenges and Legal Gaps……35

Khandokar Al Wasi [Student at American International University, Bangladesh]

5. Enhancing Cyber Forensics through Artificial Intelligence: Techniques and Challenges…….51

S. Bramanandasivam [Research scholar at Bharath Institute of Higher Institute and Research, India]

6. A Dive into the World of AI in Moulding Cybercrimes……..58

Smita Goswami [Student at Department of Law, Calcutta University, Kolkata, India]

7. Artificial Intelligence in Criminal Justice System: A Socio-Legal Analysis……..67

Pooja Narayan [Research Fellow at Faculty of Law, Teerthanker Mahaveer University, Moradabad, India]

8. The Dark Mirror of AI: Combatting the Rise of Deepfake Technologies……74

Vijpreet Pal [Student at United University, Prayagraj, India]

9. Cybersecurity in Virtual Worlds: AI-Driven Solutions for Cross-Border Jurisdictional Gaps…….80

Dr. Neeta Kumari [Freelance Academic Researcher in India]

10. Balancing Innovation and Regulation with Special Reference to Artificial Intelligence……..92

Sonal Rao [Research Scholar at Amity University, Noida, India]

Dr. Aqueeda Khan [Professor at Amity University, Noida, India]

11. Unvieling the Darknet: Cybercrimes and their Impact on Vulnerable Groups in the Digital Divide…..97

Niyathi S. and Kanigasri Vijayakumar [Student at Vellore Institute of Technology, Chennai, India]

12. Prospects Of Artificial Intelligence In Tackling Cyber Crimes…….102

Abhishek Varshney [Student at IFTM University, Moradabad, India]

13. Behind the Screen: Understanding and Countering Cyber-Terrorism in Modern Warfare…….114

Nivedita Mahesh [Student at Ramaiah University of Applied Sciences, Bengaluru, India]

14. Safeguarding Copyright Protection in AI Lead Reign: Demystifying the Enforcement through Judicial Precedents……120

Meghna Nair [LL.M. Student at Amity University Noida, India]

Dr Prabhdeep Kaur Malhotra [Assistant Professor at Amity University Noida, India]

15. Cyber Crime: Law Enforcement and Procedural Challenge……..130

Dr. Poonamdeep Kaur [Department of Laws, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab]

Prerna [School of Law & Legal Studies, DAV University, Jalandhar, Punjab, India]

16. AI and Face-Mapping Techniques in Law Enforcement: Navigating Procedural and Ethical Challenges……139

Nandana Rajesh [Research Scholar at School of Legal Studies, CUSAT, India]

17. Role of Police in Investigating Digital Crimes……145

Siddharth Baskar [Assistant Professor at IILM University, Gurgaon, India]

18. Shifting Realities: Addressing the Legal and Ethical Challenges of Deep Fakes in Indian Jurisprudence……...150

Shubhangi Pandey [Assistant Professor at SAGE University, Indore, India]

19. Addressing Online Gender-Based Violence: Legal Limitations and Human Rights Concerns in Cyber Spaces……...159

Ruthuparna M.N. and Yeshas B.S [Student at K.L.E Society's Law College, Bangalore, India]

20. Navigating Revenge Porn: Social Media's Double- Edged Sword……170

Dr. Chayanika Basu [Assistant Professor at Balaji School of Law, Sri Balaji University Pune, India]

21. AI in Indian Higher Education: Transforming Learning while Navigating Ethical and Legal Challenges……178

Matisa Majumder [Senior Legal Analyst at Contract and Compliance Management, London, United Kingdom]

Sonali Gurung [Ph.D candidate, Faculty of Architecture, CEPT, Ahmedabad, India]

22. AI-Driven Robotics: Navigating Cyber Security Concerns and the Rise of Cybercrimes……...188

Shubha M. [Student at Christ Academy Institute of Law, Bengaluru, India]

23. Integrating Artificial Intelligence and Blockchain Technology in Biotechnology: A Comparative Analysis of Patent Law and Cybersecurity Implications in India and USA……195

Avleek Dhiman [Research Scholar at Gujarat National Law University, India]
Shivansh Chauhan [Assistant Professor of Law at D.P. Vipra Law College, India]

24. Navigating the Ethical Landscape: Artificial Intelligence in Child Welfare Systems……204

Apoorwa Pandey [Research Scholar at Dr. C.V. Raman University, Kota]
Subha [Research Scholar at Bharti Vishwavidyalaya, Durg (C.G.), India]

25. AI-Enacted Cybersecurity: Strengthning Defences against Cybercrimes……213

Madireddy Divitha Reddy [Student at Christ Academy Institute of Law, India]

26. Application of IPR in Today's Fashion Industry and its Flaws……219

Kusuma Rajashekharaiah and Ananya S.B. [Student at KLE Society's Law College, Bengaluru, India]

27. Secure Transactions, Reliable Future: Unravelling the Complexities of Cybercrime in India's E-Banking Sphere……226

Asif Pasha and Milan Donson [Student at Kristu Jayanti College of Law, Bangalore, India]

28. The Role of Generative AI in Automating the Research Processes……233

Sangbit Roy and Subhayan Basak [Student at The West Bengal National University of Juridical Sciences (WBNUJS), India]

29. Implementation of Artificial Intelligence in International Aviation: A Critical Study……240

Sidhant Gupta [Assistant Professor of Law at Vellore Institute of Technology, A.P., India]

Sunavo Ray Chowdhury [Student at Vellore Institute of Technology, A.P., India]

30. Cybercrime against Women in India: A Comparative Study of Pre and Post-Covid-19 Pandemic Period……...250

Dr. Ramesh Chandra Sethi [Assistant Professor at School of Law, Kalinga Institute of Industrial Technology (KIIT), India]

Arpita Jena [Student at School of Law, Kalinga Institute of Industrial Technology (KIIT), India]

31. The Geopolitical Chessboard: AI as the New Weapon in the Arms Race……258

Shrishti Shrivas and Diksha Tripathi [Student at Narsee Monjee Institute of Management Studies, India]

32. Socio-Legal Implications of AI Integration in Courts of Justice……...265

Sudarshan Shridhar Desai [Ph.D. Research Scholar at Dept. of Law, Shivaji University, Kolhapur, India]
Dr. Vivek Yeshwant Dhupdale [Head at Dept. of Law, Shivaji University, Kolhapur, India]

33. Digital Injustice: Human Rights and the Growing Threat of Online Gender-Based Violence……..271

Pakhi Tandon [Student at Christ (Deemed to be University) Pune, Lavasa, India]

34. Cyber Crimes against Vulnerable Group: Legal Challenges and Ethical Implications……...280

Keerthana S. and Aishwarya G.J. [Student at K L E Society's Law College, Bengaluru, India]

35. Securing the Future: AI-Driven Cyber Threats, International Law, and Technological Defenses……..288

Dr. Fowmina C. [Assistant Dean cum Assistant Professor at Vinayaka Mission's Law School (VMLS), Chennai, India]

36. The Influence of Deepfake Technology and Associated Ethical Dilemmas……300

Oindrilla Ghosh [Research Scholar at School of Law, Christ (Deemed To Be) University, India]

Binod Kumar [Student at School of Law, Shri Venkateshwara University, India]

37. A Critical Study about Combating the Dark Side of AI: Deepfake Prevention through Ethical AI Development……308

Ankita Das [Research Scholar at NIMS school of Law (NIMS University Rajasthan), Jaipur, India]

Dr Manish Kumar Singh [Assistant Professor at NIMS school of Law (NIMS University Rajasthan), Jaipur, India]

38. Navigating the Cyber Frontier: Legal Challenges and Responses to Cybercrime in India……315

S. Indhu Dharshini and Jeyasri S. [Students at Sastra Deemed To Be University, Thanjavur, Tamil Nadu]

39. The Role of Artificial Intelligence in Cyber Crime……335

Mandeep Sharma [Research Scholar at Chaudhary Devi Lal University, Sirsa, India]

Nitu [LLM Scholar from Chhaju Ram Law College, Hisar, India]

40. Socio-Legal Implication of AI Integration in Courts of Justice……339

Mamta Devi [LHP College of Law, Sirsa, India]

Dr. Vikas Poonia [Department of Law, Ch. Devi Lal University, Sirsa, India]

41. E-Justice: The Role of Police in Investigating Cyber Offenses……348

Vakeel [Assistant Professor at Department of Law, Ch. Devi Lal University, Sirsa, India]

42. Protecting the Unseen – Dealing with Cyber Crimes affecting Children……354

Vishakha Agarwal and Yogita C Javkar [Student at KLE Society's Law College, India]

43. Un Convention on Cybercrime: The Concept, Concerns and Negotiations……360

Sneha M. and Pooja Shree [Student at KLE Society's Law College, India]

44. Machine Learning and Predictive Analytics as Means of Safeguards with specific reference to Artificial Intelligence and Intellectual Property Rights……...369

Dr Lisha Azeez [Associate Professor in Law cum Vice Principal, Nehru Academy of Law, India]

45. A Glance at the Role of Police in Combating Cyber Crime within the Legal Framework of India……374

Jaswant Singh [Research Scholar at Institute of Legal Stdies and Research, Mangalayatan University, Aligarh, India]

Dr Haider Ali [Assistant Professor at Institute of Legal Stdies and Research, Mangalayatan University, Aligarh, India]

46. Addressing Threats to Cybersecurity under Data Protection Laws in India: An Analysis……..380

Ashutosh Kumar Gautam [Research Scholar at Department of Law, University of Lucknow, India.]

47. Addressing Jurisdictional Challenges in Combatting Cyber Crimes: Pathways for the Future……390
Dr. Atul Jaybhaye [Assistant Professor (Law), Hidayatullah National Law University, Raipur, Chhattisgarh]

48. Digital Shadow: Social Media's Role in the Propagation and Prevention of Revenge Porn in India…...400
Lakshman Singh and Neetigya Krishna [Student at Shri Ramswaroop Memorial University, India.]

49. Role of Police in Investigating Digital Crimes……..407
Dr. Sunil Kumar [Assistant Professor of Law, Jagannath University, India]

LEGAL CHALLENGES IN CROSS-BORDER DATA TRANSFERS AMID FINANCIAL CYBER CRIMES

Nandini Braj Singh[1] and Disha Singhal[2]

ABSTRACT

*This paper, under the theme "**Law Enforcement and Procedural Challenges: Data Protection Norms and Challenges in Fraud Detection**" with the title "**Legal Challenges in Cross-Border Payments Amid Financial Cyber Crimes**", critically delves into the intricacies of cross-border data transfer regulations with respect to rising financial cybercrimes. Global interconnectedness introduces considerable challenges to data protection and security, giving rise to legal ambiguities that cybercriminals exploit. For that reason, this paper shall also evaluate the impact of data transfer on the global digital economy. This paper presents a pre-requisite description of the evolution of cybercrimes in the financial domain, starting from traditional fraud to sophisticated cyberattacks, showcasing the increasing complexity of financial crimes and regulatory bodies' subsequent difficulties in promptly addressing these issues. This study will also cater to a comparative analysis between global regulatory frameworks and India's recent legislation, Digital Personal Data Protection Act (DPDPA) 2023, to identify potential gaps in protecting financial personal identifiable information and evaluate the effectiveness of existing data protection measures in addressing cyber-oriented financial crimes and to propose potential solutions. Consequently, this paper shall provide a detailed strategy for the mitigation of financial cybercrimes in a twofold manner: Technological Solutions, such as encryption, blockchain, and multi-factor authentication; and Organizational Practices, such as Risk Management and Incident Response Planning. Further, exploring financial cybercrimes through the lens of feminist jurisprudence, this study also aims to understand whether women are equipped with coherent abilities to deal with financial cybercrimes through empirical research, employing methodologies such as questionnaires and case studies along with a narrative review. Therefore, by examining real-world case scenarios and gathering data on individual experiences, this research seeks to connect theoretical frameworks with present executive practices.*

Keywords: Cross Border Data Transfer, Cyber Financial Crimes, Sensitive Personal Data, Digital Economy, Digital Personal Data Protection, Strategy, Global Impact.

INTRODUCTION

In the interconnected world of the 21st century, cyberspace has become a platform with no tangible boundaries that binds societies from different parts of the globe together. Through this medium, information flows seamlessly across borders, transforming the traditional boundaries of communication and commerce (What Is Cross-Border Data Transfer?, n.d.). A 2020 Organization for Economic Cooperation and Development (hereinafter referred to as OECD) Report confirmed that cross-border data transfers have increased local wages and drawn greater investments in local infrastructure, thereby improving national economies and helping developing countries integrate into the global economy (Returns to Intangible Capital in Global Value Chains, 2020). Due to the prevalence of and easy access to cyberspace, cybercrimes have become an unintended consequence. The inherent greed of humans and the dependence on technology have made society vulnerable to cybercrimes of various kinds. The

[1] Student at Symbiosis Law School, NOIDA, India.
[2] Student at Symbiosis Law School, NOIDA, India.

digitalization of economies has paved paths for cybercriminals to gain illegal benefits by committing cyber-financial crimes. Cyber-financial crimes are illegal activities that are done through the medium of computers to gain some financial gain. Transnational cyber-financial crimes have become a significant risk to the global financial system's stability (Meda, 2024). Cybercriminals have found their way to abuse loopholes in the financial infrastructure, such as weak and insufficient cybersecurity frameworks, and commit fraudulent financial transactions internationally.

Cyber fraud is an umbrella that encompasses various kinds of financial crimes aimed at threatening the privacy and security of individuals as well as business entities to cause them financial losses. These include identity theft, phishing, malware attacks, and cyber-attacks on financial institutions and any criminal activity targeting financial entities and markets (Syaufi, 2023, p. 87). The advancement in e-banking and technology has accelerated the growth of cyber-financial crimes. Identity theft, one of the most heinous methods, refers to the attacker's theft of an individual's identity to use it to fraudulently take over financial accounts, like credit cards and bank accounts, to commit cyber fraud. Moreover, with the help of Artificial Intelligence, it has become easier to tailor synthetic media, called deepfakes, that further paves the way for criminals to manipulate the victim and perpetrate identity theft (Meda, 2024). In addition to causing financial loss to the victim, this also promotes the funding of unlawful activities such as money laundering and terrorism by supporting the cross-border movement of illicit funds (Syaufi, 2023, p. 87).

LEGAL FRAMEWORKS FOR REGULATING CROSS-BORDER DATA TRANSFERS

With the rising prevalence of cross-border data transfers globally, various countries have recognised the need to regulate these transfers to safeguard their citizens and industries from such financial attacks. The United States' Fair Information Practice Principles (FIPP), formulated in the 1970s, is the root of data protection principles. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 are based on accountability, minimization, quality and integrity, purpose specification and use limitation, transparency, security safeguards, openness and individual participation. Even the provisions of the General Data Protection Regulation of the European Union can be traced back to the Guidelines (Sun, 2023, 172-173).

ENSURING COMPLIANCE WITH THE GDPR

The EU's General Data Protection Regulation (hereinafter referred to as GDPR) prohibits transfers outside the EU unless the recipient country provides an equivalent level of protection. An adequacy decision is made, which involves investigating the data protection standards of the recipient country on a case-to-case basis by the EU. Once granted, an adequacy decision removes restrictions on data transfers to that country (General Data Protection Regulation (GDPR), 2016, Article 45). If a country is not covered under an adequacy decision, Article 46 of the GDPR enlists transfer tools that provide appropriate safeguards for the transfers (General Data Protection Regulation (GDPR), 2016, Article 46). They are:

- Standard Contractual Clauses- These are standardized contracts that ensure appropriate safeguards for data protection (General Data Protection Regulation (GDPR), 2016, Article 46(2)(c)).
- Binding Corporate Rules- These rules are generally adopted by companies that deal with many data transfers to ensure adequate data protection (General Data Protection Regulation (GDPR), 2016, Article 47).
- Code of Conduct- This is a set of binding rules adopted by an organization to demonstrate compliance with the GDPR. Such codes are prepared by industry representatives and are pre-approved by the data protection authorities.
- Certification- This enables data transfers to organizations that have received certification from the authority or European Economic Areas Data Protection Authorities.
- Ad Hoc Contractual Clauses- In case the data controllers or processors don't use the SCCs, they can opt for ad hoc contractual clauses that the national Data Protection Authority must pre-authorize.

Other than this, transfers can also be made utilizing Article 49, which provides derogations for specific situations, such as explicit consent, contractual performance, public interest, establishment, exercise or defence of legal claims, protection of interests of a data subject incapable of giving consent, or to provide information to the public. A necessity test is required to determine the necessity of transferring personal data for derogation, for derogation is not a rule but only an exception.

WHAT DOES DPDP HAVE TO SAY ABOUT CROSS-BORDER DATA TRANSFERS?

The Digital Personal Data Protection Act (hereinafter referred to as DPDPA) in 2023 balances the right of individuals to protect their personal data and the need to process such personal data for lawful purposes (Digital Data Protection Act, 2023, (NO. 22 OF 2023). It addresses several concerns relating to privacy, national security, and cross-border data flow. Section 16 enables the transfer of the personal data of the Data Principal by the Data Fiduciary to all countries except for those notified by the Central Government (Digital Data Protection Act, 2023, (NO. 22 OF 2023), s.16(1)). It also goes on to state that if any existing law provides for more stringent protection or restriction on transferring personal data outside India, then those provisions shall prevail over the Act (Digital Data Protection Act, 2023, (NO. 22 OF 2023),s.16(2)). This means even if the Government allows the transfer of personal data to a specific country but under sectoral laws, such transfer is prohibited for data localization purposes, then the transfer shall not be permissible. For instance, under the Payments and Settlements Act, 2007, the Reserve Bank of India has directed to localize data regarding the digital payments sector (The Payments and Settlements Act, 2007(Act no. 51 of 2007)). With this, the Indian authorities can track suspicious transactions and have quicker access to such data when investigating fraud. This also allows for greater transparency in the cross-border payments system. It also limits the ability of fraudsters to exploit regulatory gaps in other jurisdictions (Srivastava, n.d.).

Further, Section 17(1) lays down certain exemptions as to when cross-border transfers cannot be restrained in any case, such as when the processing of personal data is necessary for enforcing a certain legal right; for the performance of any judicial, quasi-judicial, regulatory or supervisory function; prevention, detection, investigation or prosecution of any offence or contravention of any law; pursuant to any contract entered; for a scheme of compromise or arrangement or merger or amalgamation of two or more companies; and to ascertain the finances of a defaulter to a financial institution (Digital Data Protection Act, 2023, (NO. 22 OF 2023),s.17(1)). The Act is also extra-territorially applicable, i.e. if any foreign entity collects personal data from India, they shall be subjected to the provisions of the Act and mandated to comply with them. However, it is pertinent to note that the Central Government has yet to come up with rules and regulations for the Act and its implementation, and only with those rules shall the application of the Act be clear.

LEGAL CHALLENGES IN CROSS-BORDER PAYMENTS

With the increase in globalisation and e-commerce, cross-border payments require multiple intermediaries on both sides, such as commercial banks, money service businesses and fintech firms, and international and domestic payment systems. Broadly, cross-border transactions involve two types of intermediaries: a front-end intermediary that interfaces with an end user and a back-end intermediary for exchanging and settling funds (Stuck in the Middle: Observations From Intermediaries in Cross-Border Payments for CBDC Design, 2021). These front-end intermediaries, such as commercial banks or other payment service providers (PSPs), depend mainly on the back-end intermediaries, such as neobanks and money transfer operators, for the transaction (Ibitola, 2023). Back-end intermediaries operate through several models, broadly classified as correspondent banking, interlinking of payment infrastructures, closed-loop, and peer-to-peer.

The role of intermediaries in cross border payments arose out of necessity to complete the steps after the user has made a command to complete a transaction, these steps help in completing the components of the transaction, making it reach the targeted location/user, therefore, forming a transaction chain. It is observed that when intermediaries have outsourced their operations to third party providers, especially for checking KYC and AML protocols have often created a loophole in this chain, thereby increasing the risk of fraud (Stuck in the Middle: Observations From Intermediaries in Cross-Border Payments for CBDC Design, 2021).

These intermediaries communicate through SWIFT messages as a security measure and to fastrack this complex transaction process. SWIFT, even after being a highly secured network, depends on the credibility of its participants for its security (There Is No Alternative: SWIFT as Infrastructure Intermediary in Global Financial Markets, 2019). Participants who are weak in terms of following their cybersecurity measures, lead a pathway for cyber criminals to use the transaction chain they are working on, to commit financial fraud (NELSON, n.d.). When working through a centralised system, which requires a large amount of intermediaries, layers are built, increasing the complexity of the chain, hence, making the origin of the transaction, harder to trace. This challenge arises due to the fragmentation of the information among intermediaries across jurisdictions (Meli & Baer, 2023).

Unauthorized SWIFT messages through compromised intermediary banks in the transaction change is yet another challenge for cross-border transactions, as this approach if often used to hack their systems, send fraudulent messages through these compromised systems and further instructing the transfer of funds to illegitimate accounts,increasing the risk for fraud and money laundering(How Banks Are Combating Cyber Attacks on Their SWIFT Payments, n.d.). The Bangladesh heist in 2016, is a key example of how vulnerabilities in an intermediary institution's security can lead to a large- scale fraud. This heist was successful using fraudulent messages sent via SWIFT, leading to a loss of $81 million(Bangladesh Hack Illustrates Rising Sophistication of Attacks, n.d.).

JURISDICTIONAL CHALLENGES

Jurisdictional challenges are exacerbated in cybercrime cases, especially in cross-border payments, because perpetrators often operate across multiple borders, and their attacks may be launched from jurisdictions that do not cooperate with international investigations. Fraudsters frequently exploit jurisdictions with weak or non-existent cybercrime laws, like countries with low AML and KYC compliances, which includes Iran and Monaco etc. or lenient regulation over the SWIFT network, like Lebanon and Panama, to target financial institutions in other countries. This methodology is often referred to as Regulatory arbitrage (High-Risk Third Countries for AML Purposes, n.d.).

This challenge further increases with the current adaptation towards DLT-like Blockchains, which reduces the need for centralized intermediaries in the transaction process but as being a developing and innovative solution, many countries are yet to decide on their regulations (MORGAN, n.d.). With the increase in the use of digital assets, cryptocurrencies, and decentralized finance (DeFi), regulatory arbitrage is becoming common when users leverage jurisdictions with relaxed rules on these emerging technologies to conduct illegal transactions, including fraud, with relative anonymity (Recommendations for Regulating and Supervising Bank and Non-Bank Payment Service Providers Offering Cross-Border Payment Service, n.d.).

Regulatory arbitrage has led to two major developments in Fraud:

1) Fraud through Layering and Obfuscation: Regulatory arbitrage is often used by fraudsters to complex the structures in the transaction process, which disrupts the origin of the transaction for example, if a fund is being transferred from one place to another, the place of origin of the funds may never be traced due to such high complexities inserted in the channel. This makes tracing & auditing transactions difficult (The 3 AML Stages: Layering, Placement, & Integration Explained - Blog, 2024).
2) Fraud via Jurisdiction Shopping: Often hiding behind shell companies, Fraudsters participate in business transactions between jurisdictions with lenient laws for payment systems and further registration procedures, choosing jurisdictions freely to transfer or steal money from once they set up their bases at a weaker regulated place (Illicit Financial Flows From Cyber-Enabled Fraud, n.d.).

MITIGATION STRATEGIES

Long Transaction Chains and involvement of intermediaries raised concerns all across the world. They led to the development of the SWIFT network with additional features and DLT Technologies as described below:

Mitigation Efforts Through SWIFT:

End-to-End Payment Tracking (SWIFT gpi): SWIFT gpi improves transparency and real-time tracking, providing better oversight of transactions as they move through intermediaries (Delivering Added-Value, n.d.).

Customer Security Programme (CSP): SWIFT's CSP requires participating institutions (including intermediaries) to strengthen their cybersecurity posture, mitigating the risk of fraud through hacking or unauthorized access to SWIFT systems (Customer Security Programme (CSP), n.d.).

Fraud Detection Tools: SWIFT also provides tools like Sanctions Screening and Payments Data Quality services that help financial institutions, including intermediaries, detect and prevent illicit transactions that may be part of fraudulent schemes (Swift and Global Banks Launch AI Pilots to Tackle Cross-Border Payments Fraud, 2024).

KYC and AML

KYC is a process for verifying individuals before they participate in any sort of cross-border payments, whereas AML regulations help in monitoring payment patterns that are suspicious, both helping in the early detection of fraudulent transactions like money laundering.

Multi-Factor Authentication

MFA is a security feature that scales up protection efforts by mandating that users provide two or more verification methods. For instance, a combination of a passcode and mobile identity is one of the most potent tools applications can use to make it hard for hackers to enter financial systems. It adds another layer of security which ensures that any kind of unauthorised access is prevented even if one security factor (like a password) is compromised without the second authentication factor.

Real-time monitoring and AI-based fraud detection

AI-based security has been proven to be fruitful, especially in identifying abnormalities in patterns of transactions that may be risky, which may include large transfers to unfamiliar accounts, sudden spikes in activity, or transfers to high-risk jurisdictions(Tennant, n.d.).

AI-based security systems even send real-time notifications to the transactors, which prevents any damage to sensitive financial data and provides fast and secure cross-border transactions. Real-time monitoring using AI and training these machines using historically collected data allows for the immediate flagging and halting of suspicious transactions, preventing fraudulent activities from being completed.

D.L.T.

Distributed Ledger Technology is a system that is decentralised in nature, where transaction participants

have access to the same records in a synchronised manner, maintaining transactions in a secured channel protected by cryptography(GAO-19-704SP, Science & Technology Spotlight: Blockchain & Distributed Ledger Technologies, n.d.). This reduces the need for intermediaries and mitigates any security risks they pose. One of DLT's main features is immutability, as once data is stored in this decentralised mechanism, it is hard to alter such data(World Bank Document, n.d.). There are various types of DLT, but one of the emerging ones is blockchain.

Blockchain Technology

Blockchain is a technology which, instead of sending data collectively in a centralized manner across the transaction chain requiring multiple intermediaries to receive it, only records transactions in a decentralised manner in smaller units called “blocks” connected in “chain” like channel across multiple locations each time in a unique pattern, This makes the procedure of sending and receiving money easy and quick. This process, being decentralised, also does not require intermediaries in the transaction chain; therefore, it is considered a user-friendly and peer-to-peer transfer (How DLT, APIs, and CBDCs Are Changing Cross-Border Payments, 2024). Blockchain technology helps increase transparency and security in cross-border transactions. This is because each transaction is recorded and sent across in a unique manner, which is difficult to alter without the consensus of the network. Such unique and secure transactions, which are also easily traced, further aid in detecting fraudulent activities before any major losses like money laundering or cyber terrorism.

Encryption

Encryption, if understood from an analogy, puts our sensitive data under a lock as soon as we transmit it, allowing only the one to whom it is sent, with a key, can decrypt it, which means that until the target is reached, no one can access the information in the transaction channel. For cross-border payments, encryption locks away all the sensitive information of the payer, making the transaction secure compared to other means, which reduces the risk of fraudulent activities in the transaction channel.

Risk Management in Cross-Border Payment Frauds

Organisations in the current digital era often invest in a dedicated and independent Fraud Control unit equipped with professionals with experience in fraud detection and risk management using mitigation strategies discussed above in this paper. Industries Today, while providing training to their employees for their respective fields, ensure that risk management training becomes a part of it, which helps develop precautionary measures for financial fraud. It is suggested to organisations that cybersecurity professionals undertake risk assessments to address any vulnerabilities that may arise in multiple transactions exercised by firms every day. Moreover, Proactive measures such as fraud simulation testing and advanced analytics integrated with machine learning can help detect weaknesses in the present infrastructure of the organisation (Combating Fraud in the Era of Digital Payments, n.d.).

Incident Response Planning in Cross-Border Payment Frauds

Incident Response Planning is a matter of internal grievance redressal mechanism of an organisation,

which is generally dealt with by the Fraud Control unit by experts in fraud cases and cybersecurity. Incident response planning is constantly upgraded as per the emerging technologies, such as the shift to blockchains, the preparation for risks attached to it, and timely reports to senior management to critically evaluate the organisation's preparedness to detect fraudulent activities. Customer awareness programs are vital apart from building a response team to educate customers on the risk of digital transactions and safety protocols. Adding to this, the setting up of mechanisms and detailed procedures helps in the quick detection of fraud. Currently developed technologies like resistance AI work at an advanced level, ensuring real-time monitoring and checking the legitimacy of the devices. At the same time, regulatory frameworks guide the compliance efforts of financial institutions (FIs)(Combating Fraud in the Era of Digital Payments, n.d.).

CASE STUDY

To discuss how societal structures of gendered roles and financial independence interlink with the vulnerabilities of women to financial cybercrimes, the authors have conducted a survey in a sample size of 100 women.

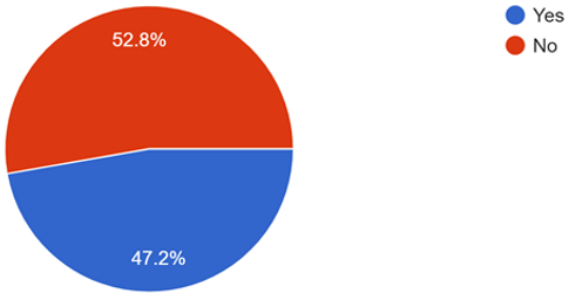


Figure 1. Have you ever received financial literacy training (formal or informal)?

Survey results suggest that even after 47.2% of women have received financial literacy training, they are more susceptible to financial cybercrime largely due to lower financial independence and lack of awareness. Financial independence, in this context, is not an individual matter but rather a function of broader social, economic, and legal infrastructure.

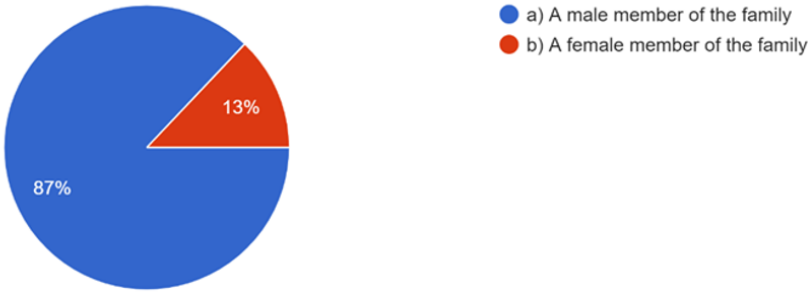


Figure 2. If you have been a victim to cyber financial crimes, who do you go to seek first-hand advice from?

Interestingly, the study finds that 87% of female victims consult their male family members for advice because they feel men are better placed to understand the transactions, hence reinstating the stereotypical gender roles that restrict the right of women to act independently in financial affairs. Legal systems must first work to rebalance these power dynamics by providing equal access to financial tools and helping an environment where women feel empowered to make independent decisions over their finances in order to arm women with coherent abilities to deal with financial cybercrimes. That includes not only financial literacy but also some tearing off of societal expectations that would discourage women from really engaging intimately with financial systems. The two salient reasons for women's over-exposure to financial cybercrimes that the survey fetches are unfamiliarity and scams targeted at the gender. This follows from the systemic exclusion of women from platforms where financial education and decision-making are conducted. In most societies, women remain without equal access to financial literacy programs. This lack provides a gap between their preparedness to handle financial risks across genders. Suggestions, made by some of the participants themselves, include awareness programs for cybersecurity and financial independence so that they build confidence in handling their finances and be less susceptible to such frauds. Thus, based on this survey, it can be determined that women are educated and formally trained. However, societal norms and economic inequalities hold them back as coherent abilities to deal with financial cybercrimes. Women's Empowerment in this space must come through legal reforms and cultural changes toward true gender equality in financial autonomy and cybersecurity.

CRITICISM OF THE DPDPA

Following the 2017 judgement of Justice K.S. Puttaswamy and Anr. v. Union of India and Ors., where the right to privacy was recognised as a fundamental right, the government constituted a committee chaired by Justice B N Krishna to recommend a proper legal framework for data protection (Greenleaf, 2018). The Committee, in its report, recommended forbidding cross-border transfers of sensitive personal data due to historically unregulated transfers leading to violation of privacy and unlawful processing (Srivastava, n.d.). It is intriguing to note that initial drafts of the DPDPA distinguished between critical and sensitive personal data, but the same cannot be found in the DPDPA. This distinction was essential for data protection and localization. However, now it may be on the discretionary power of the Government to notify on a case-to-case basis (India: Digital Personal Data Protection Act, 2023 - What It Means for Cross-Border Transfers, 2023). The Act is also silent on further transfers of data, therefore, creating a vacuum, i.e. a company belonging to a blacklisted country may obtain data from a company belonging to a non-blacklisted company.

With respect to Section 16 (1), the Act does not specify the grounds for restricting the transfer of personal data to a country notified by the Government (Digital Data Protection Act, 2023, (NO. 22 OF 2023),s.16(1)). The Act does not prescribe any adequacy check or security requirements that the Data Recipients and Data Fiduciaries should maintain, nor any adequate safeguard agreement format to execute with the Data Recipients to process the data. Moreover, it is not clear whether or not Data Recipients will be notified by the government if their laws are appropriate or not for such transfers. It may be clearer once the government releases the rules for DPDPA, which will detail the adequacy

checks that need to be carried out for cross-border data transfers (Srivastava, n.d.). The provisions of the Act on the restriction of data transfers lack specificity and clarity, which may expose an individual's personal data when it is being sent to countries with significantly weaker data protection laws. It has been further argued that the Data Protection Board may not be independent and effective due to its short-term appointments, which may portend bias or even external influences.

RECOMMENDATIONS

Considering the overall research in this paper, the following recommendations are proposed:

- Criteria for evaluating countries have to be made strict and detailed with standards that protect the personal data of Indian citizens effectively, apart from the cross-border transaction data that is regulated by RBI.
- Real-time fraud detection systems, both as precautionary measures and cyber forensic tools, have helped in mitigating fraud with their constant development of machine learning and Artificial Intelligence for monitoring suspicious transactions; if applied uniformly globally, along with systems like SWIFT, Fraud detection can become much simpler and easier in the future days.
- Conducting risk assessments at periodic intervals is necessary, and providing a report to the Data Protection Board would bring accountability in protecting data leaks and further help in understanding areas where data is more vulnerable to leaks.
- Introduce an adequacy decision mechanism similar to GDPR, which allows transfers to countries with adequate levels of data protection. This system can ensure that personal data transferred outside India will be treated with similar safeguards. India needs inspiration from an adequacy decision mechanism similar to GDPR, which permits transfers to countries with a high-security standard for data protection. This mechanism will ensure that the personal data of Indian citizens transferred outside India will be treated with similar precautions.
- India, being a highly populated country, must work towards building a risk-based approach similar to Singapore's PDPA, which has clear demarcation for the transfer of data based on the amount of risk posed by the receiving country.
- An amendment can be made to the DPDPA of India to insert a certification mechanism specifically for data fiduciaries and other cross service providers who process sensitive data involved in cross-border payments.
- Maintenance of an audit trail for cross border transactions in each organisation for keeping a verified record of data transfer, shall be made accessible to for investigations to inquire for cases of fraud and other cyber security breaches by amendment as a mandate under Section 16 of the DPDPA.

CONCLUSION

After thoroughly analyzing all the literature, we conclude that financial cybercrimes require keen attention at both national and international levels, where countries need to strengthen their cyber security laws to reduce fraudulent activities in their jurisdiction. Concerning India, though DPDPA has

been proven to be fruitful for a blanket Data Protection outlook, it still requires amendments to deal with cross-border data transmission in the complete sense, including cross-border payments, which may not come easy as they must comply with the PMLA and RBI's directives for cross border payments. Regulatory Arbitration has been seen as a big issue that requires uniform global attention with treaties and the implementation of cross-border regulations to prevent fraudulent activities. The boom in technology like blockchain encryption and AI also serves in the best interest of the cyber security and cyber Forensic dimensions to mitigate fraud efficiently.

While the above is catered to, it is also vital to keep a check on making such strategies gender sensitive as the case study submitted in this paper suggests that women feel underconfident to tackle financial cybercrimes independently while some suggest that they prefer or trust a male member of the family to deal with such risks or circumstances with reasoning that they are more qualified to deal with the same, creating a strong need for increasing financial security literacy for women for them to be truly independent which will be supported by government initiatives and gender sensitive approach towards the policies and laws making them accessible for all.

*****

REFERENCES

1. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. OJ L 119, 4.5.2016, p.Art. 45 GDPR – Transfers on the basis of an adequacy decision - General Data Protection Regulation (GDPR)
2. Digital Personal Data Protection Act (DPDP Act), No. 22 of 2023, India Code (2023). https://www.indiacode.nic.in/bitstream/123456789/24073/1/dpdp_act_2023.pdf
3. The Payments and Settlements Act, 2007(Act no. 51 of 2007) https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf
4. The 3 AML Stages: Layering, Placement, & Integration Explained - Blog. (2024, May 16). Unit21. Retrieved October 23, 2024, from https://www.unit21.ai/blog/3-stages-of-money-laundering-placement-layering-integration
5. Bangladesh hack illustrates rising sophistication of attacks. (n.d.). KPMG. Retrieved October 23, 2024, from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/08/swift-it.pdf
6. Combating fraud in the era of digital payments. (n.d.). PwC India. Retrieved October 23, 2024, from https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf
7. Customer Security Programme (CSP). (n.d.). Swift. Retrieved October 23, 2024, from https://www.swift.com/myswift/customer-security-programme-csp
8. Delivering added-value. (n.d.). Swift. Retrieved October 23, 2024, from https://www.swift.com/our-solutions/swift-gpi/swift-gpi-banks/delivering-added-value

9. GAO-19-704SP, Science & Technology Spotlight: Blockchain & Distributed Ledger Technologies. (n.d.). Government Accountability Office. Retrieved October 23, 2024, from https://www.gao.gov/assets/gao-19-704sp.pdf
10. Greenleaf, G. (2018, July 27). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B. MeitY. Retrieved October 23, 2024, from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
11. High-risk third countries for AML purposes. (n.d.). The Law Society. Retrieved October 23, 2024, from https://www.lawsociety.org.uk/topics/anti-money-laundering/high-risk-third-countries-for-aml-purposes
12. How Banks are Combating Cyber Attacks on Their SWIFT Payments. (n.d.). Eastnets. Retrieved October 23, 2024, from https://www.eastnets.com/white-papers/how-banks-are-combating-cyber-attacks-on-their-swift-payments
13. How DLT, APIs, and CBDCs are Changing Cross-Border Payments. (2024, May 6). Opus Technologies. Retrieved October 23, 2024, from https://opustechglobal.com/how-dlt-apis-and-cbdcs-are-changing-cross-border-payments/
14. Ibitola, J. (2023, April 18). Preventing and Stopping Fraud in Cross-Border Payments. Flagright. Retrieved October 23, 2024, from https://www.flagright.com/post/preventing-and-stopping-fraud-in-cross-border-payments
15. Illicit Financial Flows from Cyber-Enabled Fraud. (n.d.). FATF. Retrieved October 23, 2024, from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf
16. India: Digital Personal Data Protection Act, 2023 - what it means for cross-border transfers. (2023, November 02). Onetrust Data Guidance. https://www.dataguidance.com/opinion/india-digital-personal-data-protection-act-2023-what
17. Meda, K. (2024, May 3). Identity theft is being fueled by AI & cyber-attacks. Thomson Reuters. Retrieved October 23, 2024, from https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/
18. Meda, K. (2024, May 3). Identity theft is being fueled by AI & cyber-attacks. Thomson Reuters. Retrieved October 23, 2024, from https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/
19. Meli, M., & Baer, J. (2023, March 31). Unmasking the hidden dangers: How cyber threats target intermediaries. Julius Baer. Retrieved October 23, 2024, from https://www.juliusbaer.com/en/business-navigator/technology/unmasking-the-hidden-dangers-how-cyber-threats-target-intermediaries/
20. Meltzer, J. P., Qureshi, Z., & Jeong, D. (2018, March 20). Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia. Brookings Institution.

Retrieved October 24, 2024, from https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/

21. MORGAN, J. (n.d.). Cross-border payment modernization. J.P. Morgan. Retrieved October 23, 2024, from https://www.jpmorgan.com/payments/payments-unbound/volume-3/cross-border-payment-modernization
22. NELSON, A. (n.d.). The Global Cyber Threat to Financial Systems – IMF F&D. International Monetary Fund (IMF). Retrieved October 23, 2024, from https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm
23. The Payments and Settlements Act. (2007). Universal.
24. Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Service. (n.d.). Financial Stability Board. Retrieved October 23, 2024, from https://www.fsb.org/uploads/BAFT.pdf
25. Returns to intangible capital in global value chains. (2020, September 30). OECD iLibrary. Retrieved October 24, 2024, from https://www.oecd-ilibrary.org/trade/returns-to-intangible-capital-in-global-value-chains_4cd06f19-en
26. Srivastava, S. (n.d.). India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL. Indian Journal of Law and Technology. https://www.ijlt.in/search-results?q=India%3A+Decrypting+critical+concepts+under+India%27s+Digital+Personal+Data+Protection+Act%2C+2023+and+com
27. Stuck in the Middle: Observations from intermediaries in cross-border payments for CBDC design. (2021, August 1). Bank for International Settlements. Retrieved October 24, 2024, from https://www.bis.org/events/cpmi_ptfop/proceedings/paper11.pdf
28. Sun, L. (2023, November). Overview of Regulations on Cross Border Data Flow. Academic Journal of Science and Technology, 8, 172-173. https://www.researchgate.net/publication/375855814_Overview_of_Regulations_on_Cross_Border_Data_Flow
29. Swift and global banks launch AI pilots to tackle cross-border payments fraud. (2024, May 30). Swift. Retrieved October 23, 2024, from https://www.swift.com/news-events/press-releases/swift-and-global-banks-launch-ai-pilots-tackle-cross-border-payments-fraud
30. Syaufi, A. (2023, June). Employing Forensic Techniques in Proving andProsecutingCross-border Cyber-financial Crimes. International Journal of Cyber Criminology, 17(1), 87. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/150/55
31. Tennant, F. (n.d.). Cross-border payments: fraud mitigation strategies — Financier Worldwide. Financier Worldwide. Retrieved October 23, 2024, from https://www.financierworldwide.com/cross-border-payments-fraud-mitigation-strategies

32. There is no Alternative: SWIFT as Infrastructure Intermediary in Global Financial Markets. (2019, January 21). FinGeo. Retrieved October 23, 2024, from https://www.fingeo.net/swift-as-infrastructure-intermediary-in-global-financial-markets/

33. What is Cross Border Data Transfer? (n.d.). Securiti.ai. Retrieved October 23, 2024, from https://securiti.ai/glossary/cross-border-data-transfer/

34. World Bank Document. (n.d.). World Bank Document. Retrieved October 23, 2024, from https://openknowledge.worldbank.org/server/api/core/bitstreams/5166f335-35db-57d7-9c7e-110f7d018f79/content

*****

CYBERSECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE: TWO MAJOR FORCES BEHIND THE CREATION OF CRIMINOGENIC SOCIETY GLOBALLY

***Maitri Shail Patel*[3]**

ABSTRACT

*Every society and societal thinkings have undergone an evolutionary change over a long period of time since the terms like "**civilization**", and "**society**" have been recognized in the several parts of the world. There have been several anthropogenic studies as well as detailed researches on various aspects which have revealed that the societies all over the globe have become "**criminogenic**" as in driven by the behaviour like that of hardened criminals where people tend to indulge in criminal activities to achieve their gruesome goals and fulfil their deepest & darkest desires marking the end of law, justice as well as humanity. There have been major factors and multi-dimensional forces responsible for the creation of such a menacing as well as troubling scenario of creation of criminogenic societies that are being experienced by the people every now and then. It is however, noteworthy that the two major forces which have contributed significantly in the creation of criminogenic societies all over the world are: **cybersecurity concerns** and **use of artificial intelligence (AI).** It sounds very shocking or rather astounding that cybersecurity concerns and use of artificial intelligence are the two most major contributors in the creation of criminogenic societies but it's a fact that has been experienced magnanimously by the large number of the people all over the world as the everyday life has become really too dependent on technological advancement and even on the use of artificial intelligence. Until now, a lot researches have been conducted on cybercrimes and artificial intelligence. But the need of the hour is to study the socio-psychological as well as socio-legal aspect of cybersecurity as well as artificial intelligence altogether to understand that how the societies have reached here so far from what these used to be (i.e., so, far from imagination or any kind of speculation by anyone). Even the way the severity of crimes has increased, its all because of the easy access to the latest technology that's being misused as well as abused to carry out the same. With such a scenario, law, justice, and rights of the people have become endangered of being extinct. The challenge for the law-makers as well as the law-enforcers have also henceforth increased manifold. This research paper focusses on the contributions of cybersecurity concerns and use of artificial intelligence in creation of criminogenic societies globally beginning from how it actually started and then took the form in which it currently is. Also, the paper will attempt to come up with some practical solutions to this "**dual problem**" with deeper insights to the recent problem.*

Keywords: Criminogenic Society, Cybersecurity Concerns, Artificial Intelligence, Dual Problem.

HISTORICAL BACKGROUND: DETAILED INTRODUCTION TO THE STUDY

Cybersecurity and **Artificial Intelligence** have been the most researched, discussed, debated, invented, innovative and the creative topics and areas of knowledge which have captured the deepest interests of billions of intellectual people from various field be it engineering & technology, fashion designing, photography, medicine, and even law and other fields all over the world including several professionals from each such field from India too, who have created their careers and professions surrounding either one of them or both of them altogether. Especially, the youth and even the generation next to **the Gen Z** which are being brought up by their mothers with the use of lullaby from YouTube and other internet

[3] Ph.D. Student at GLS University (Ahmedabad), India.

hacks unlike the mothers of the people from earlier generations several decades back as in from **40's-50's till 90's-2000's** mothers. Even the way the fathers of generations after Gen Z managing and nurturing their families have become totally different from the earliest of the generations since 40's till 2000's.

Alongwith the burgeoning effects of both the **cybersecurity concerns** and **usage of artificial intelligence**, the most dangerous threat looming over the very existence of humanity and the sociological concept of society is the fact that with such dual advancement taking place exponentially, the societies all over the world have become **"Criminogenic"**, as in full of such a toxic environment which is making every sane individual including the teenagers, youth, and even middle-aged people as well as the old-aged people to indulge themselves in committing heinous, gruesome, severe and grave inhuman crimes for getting their whims, desires, ulterior motives, greed and revenge on anyone rather than focussing on the power of hard work, virtues, self-realization, meditation, spirituality and humanity. Every moment, every day there's such a criminal case which make all the people wonder and think while questioning in an insightful way: "What kind of progress the humans are moving towards? What are societies becoming day by day? Where would it end? ….and other such endless questions making everyone's faith and beliefs to shake tremendously.

The Indian scenario combined with the International Scenario needs to be henceforth studied to understand this current problem involving not only the Indian society but every society in the world to be forced to be criminogenic society due to the dual force of increasing cybersecurity concerns and use of artificial intelligence almost in everything which has sparked the major concern of the fear of extinction of human intelligence just like the cinematic depictions of this scenario in the famous Rajnikanth and Aishwarya Rai Bachchan starrer Telugu movie named "Robot"; then, in the Hollywood movie titled "the Transformers" movie; Akshay Kumar starrer Tamil movie "2.0" and Shahid Kapoor-Kriti Sanon starrer Bollywood movie "Teri Baaton Mein Aisa Uljha Jiya" and so on.

A detailed study on cybersecurity & its concerns and artificial intelligence & it's usages and then, a combined study on both in Indian perspective as well as the International/Global perspective can really be insightful, helpful as well as resourceful for understanding the factors responsible for initiating the vicious cycle of the formation of such criminogenic societies all over the world and making maximum people understand it before it's too late.

CYBERSEURITY AND ALLIED CONCERNS

Cybersecurity, as all people are hyperaware nowadays, is a very dynamic, ever-evolving and a very troubling concept that has come into existence with time as the usage of internet increased almost exponentially with its advent. There have been various discussions, talks & debates, legal considerations, researches, studies and investigative documentations regarding various allied concerns of cybersecurity like: (1) Cybercrimes; (2) Cyberstalking; (3) Cyberbullying; (4) Usage of Cyberspace; (5) Hacking: (6) Phishing; (7) Cyber Terrorism; (8) Cyber Espionage; and all the other emerging concerns with the growing use of cyberspace, and advanced technologies.

When it comes to the meaning of the term 'cybersecurity', it has always been mentioned that it's infinite and enormous size have actually created a way for multiple interpretations making it a very subjective aspect. There's no fixed meaning for it. The meaning is decided as well as determined by the users of the cyberspace be it those utilize internet spaces and various domains as online gamers, researchers, professional academicians, hackers, bloggers, social media influencers, tech savvy people, computer science students & professionals, software & hardware engineers, website/domain owners, businesswomen as well as businessmen and various others.

Now, the need of the hour is to brainstorm and list down all the possible meanings of the term cybersecurity; compile them; conceptualise it for law-making, mitigation of cybercrimes and ensuring the safety of data and virtual life everyone on social media platforms as well as websites and various online gaming servers and work websites. The subjective and diverse nature of cybersecurity needs to be embraced wholeheartedly for arriving at a conclusive, comprehensive, accurate and a precise meaning. Also, there's a requirement of the coining as well as recognition of yet another term which is **"Cyberdiversity"** which basically means etymologically, the diversity of usage and users of cyberspace.

When it comes to defining the term 'cybersecurity', well, it's mostly defined in some fixed contexts like cybercrimes, safety on the internet, data security, protection & safeguarding of sensitive data and so on. But there's a lack of an in-depth definition of cybersecurity. To be very clear, it will be absolutely correct to mention that as compared to cybersecurity, the term "cybercrime" has become the most google searched, researched, studied, debated, discussed and the paramount concept while the truth is that it's just a tiny unit, a mini facet and a little aspect under cybersecurity.

To make everyone understand what actually the cybersecurity is, it needs to be defined in an original, observant, innovative, dynamic and a more realistic manner. So, saying that, the term 'cybersecurity' can be defined as: **"The extent to which all kind of data are safe and secure from any kind of theft or harm on the diverse cyberspaces is termed as Cybersecurity."** Although, this definition appears to be simple, it's a step ahead towards getting deeper into it while exploring its areas and contours to understand it and its allied concerns with efficiency, precision, and accuracy.

The concept of cybersecurity originated much later than that of cybercrimes and cyberattacks alongwith it's much later recognition. Just like in every story where the cities develop and then, they are planned by the town planners instead of town planning first and then, creation of cities, the cybercrimes and cyberattacks came into limelight and then, the concept of cybersecurity was recognized. The evolution of the concept of cybersecurity has happened mostly after 2017 when it was recognized in the developed countries first and then, in the developing as well as the underdeveloped countries and especially, after the exponential increase in the accessibility to the cyberspace with data plans in affordable prices all over the world alongwith the supremely increased use of cyberspace all over the world for even the tiniest task. The various aspects of cybersecurity have been evolving since then with the various aspects and extents of data protection, security and safety on the cyberspace in any way.

Apart from cybersecurity, the allied concerns that have been surfacing recently are Cyber Violence, Cyber Terrorism, Cyber War, Cyber Espionage and Cyber Defence. These are the tip of the iceberg of the deeper issues that are seeping in all over the world in one way or the other. Also, surprisingly, these concerns are no more alien or unknown to the people as using cyberspace has become a new-normal since a long time as in more than a decade ago.

- CYBER VIOLENCE: It is another recently originated and evolved term which is one of the most challenging concerns allied with the cybersecurity. The term "cyber violence" basically, means using cyberspace for attacking someone's dignity or data causing an emotional hurt or a mental trauma for altruistic and selfish motives.
- CYBER TERRORISM: As the term suggests, it's about misusing and abusing the accessibility of the diverse cyberspace for creating a terror and havoc amongst the masses of public causing severe data harm as well as psychological trauma leading to devastation of integrity and security of several nations all at once.
- CYBER WAR: Nowadays, the cyberspace is not being used only for creative ways but also, in a highly destructive manner as in fighting psychological wars for hacking into other countries' firewalls and secured domains to steal the sensitive and secret information with a malevolent intention of misusing the weaknesses against them for making them crippled and disabled. The wars that are nowadays, fought on the cyberspace with even more evil strategies and cruel tactics are known as Cyber War.
- CYBER ESPIONAGE: The companies' data including its trade secrets, intellectual property protections, and other sensitive data are being attacked, stole, misused and used cruelly for removing them out of the corporate competition. This is termed as Cyber Espionage.
- CYBER DEFENCE: It is a term which refers to the ways of defending one's cyberspaces for ensuring safety, security as well as the protection of the data smartly, strategically and efficiently.

ARTIFICIAL INTELLIGENCE (AI) AND IT'S USAGES

Artificial Intelligence (AI) as the term suggests, it **means** artificially created, developed, curated algorithms and are altogether compiled in a way to create an intelligent and smart beings by the human beings themselves. Also, it can be simply and generally **defined** as: **"a perfect blend of artificially curated algorithms, programmed intelligence, high-tech software and a capability of acquiring other intelligence on its own and which have been developed for making the lives of all the humans easy by reducing their workload, and saving their time, money, and energy."**

Artificial Intelligence has been in exponential use at a global level since it's origination in the developed nations like China, Japan, U.S.A., and others. This technological advancement has been utilized at a deeper level in the developing countries and especially, in India since the first robotic advanced surgery happened in the **All-India Institute of Medical Sciences (AIIMS), New Delhi** in the first time in the **year 2006**. The surgery was performed by **Dr. Prem Nath Dogra**, a urologist, who used a four-armed

robot. The surgeon monitored the robot using a surgical console, similar to an airplane pilot in a cockpit.

Here are some other milestones in the history of robotic surgery in India:

- **2000**: The FDA approved the da Vinci system for urologic robotic surgery
- **2007–2017**: A decade of rapid growth in robotic surgery in India
- **2023**: 66 robotic surgery centres in India, 71 robotic systems installed, and over 500 doctors trained in robotic surgery

Robotic surgery is used in a variety of medical fields, including urology, gynaecology, orthopaedics, laparoscopy, thoracoscopy, and arthroscopy.

Not only this, but even the search engines that we use on our PCs, Laptops, Desktops, iOS cellphones, and Android Smartphones like Google Chrome, Microsoft Edge, Mozilla Firefox, etc. not only make our research study, our search for the required any kind of information as well as the collection and data compilation easier than ever. Also, they are one of the several forms of artificial intelligence at work where these search engines store every detail about the users and based on it's search history and interests, it designs their personal news feed and even newer search recommendations.

Similarly, the shopping apps like that of Myntra, Amazon, Meesho, Zepto, Blinkit, Big Basket, Swiggy Instamart, etc. too, collect the information based on users' search and shopping history and send the regular notifications about the suitable shopping schemes luring to keep shopping often and often. Even the cars are nowadays laced with all advanced and artificially intelligent features like the 360-degree cameras to check out the traffic in all 4 directions at once without causing spondylitis as in pain the neck at all and self-drive mode or auto-drive mode for longest car trips ever in any place in the entire world.

The traceability of every human being in any part of the world has become very easier than before as anyone can be located precisely with the help of the Global Positioning System (GPS) that's the default feature in almost all the android as well as iOS smartphones and also in most of the food delivery apps, shopping apps, Internet Search Engines, Google Timeline Features and all the Social Media Apps like the Instagram, Facebook, Snapchat, X (Twitter), and so on. It's all a big thanks to the advancement of artificial intelligence over a long period of time.

The artificially intelligent electrical gadgets like the hairstyling machines and the dry as well as wet vacuum cleaners manufactured by the most renowned company named Dyson alongwith the Robotic Cleaning Machines and Smart Machines for cleaning which have not only eased the burden of household work but also have revolutionized the conventional lifestyle of most of the human beings nowadays. Also, the wave of digitalization of banking, payments, finances and transactions which boomed from India in the form of UPI through various platforms like Paytm, PhonePe, etc., and so on, has taken a massive and an enormous form as it's webs have spread far and wide throughout the globe, is also, another form of artificial intelligence in action.

Apart from almost infinite number of usages, the advancement as well as the development of artificial intelligence, a lot of hot and debatable questions having the scope of various futuristic researches like: "Will artificial intelligence be taking over the human intelligence? Will the world have a dramatic, shocking yet a really devastating ending as shown in the "Transformers' Movies?" ….and so on. Also, the artificial intelligence has been discovered as being one of the two major forces alongside cybersecurity concerns responsible for the criminogenic society every passing moment, and every day. Let's study and understand in-depth as to how is that possible and think of something to solve this hovering menace for the future.

FORMATION OF A CRIMINOGENIC SOCIETY EVERY MOMENT & EVERY DAY: REALITY CHECK AND AN IMPORTANT CONCLUSION ALTOGETHER

The term **"Criminogenic"** means as "in something of a criminal, or an illegal nature" therefore, a **"Criminogenic Society"** can be precisely defined in a general norm as "a society where people are driven by their malafide intentions and malevolent intentions to achieve their end goals by indulging in committing crimes, illegal acts as well as the offences just for the sake of their emotional satisfaction in the form of revenge, greed, etc., and so on."

Nowadays, with the multi-variate and the exponential development as the advancement of technology in almost all possible aspects possible or even unimagined 3-4 decades ago, there have been several factors behind the conversion of the current society into a criminogenic society globally out of which the two major forces which have led to the creation of this most futuristic and a challenging problem are: **Cybersecurity & Allied Concerns** and **Artificial Intelligence & It's Usages.**

Actually, the advancement of Artificial Intelligence (AI) with the creation of various pathways for commission of the most severe, heinous, gruesome, and inhumane cybercrimes with the creation of artificial bots as in artificial humans, with fake identities as real as the natural humans which can lead to problems in tracing the real offenders as well as the criminals and such things happen on the infinite cyberspace as it is misused in several ways apart from being used in various ways as mentioned in the earliest section of this research paper.

Easy accessibility of the enormously infinite cyberspace in the form of reasonable data plans have actually been very conducive for the misuse of artificial intelligence which does not necessarily have to be devastating and destructive as contrary to the original intention behind the creation as well as the development in this direction when it actually began in the late 2000's and especially, later than the year 2014.

The dual forces of Artificial Intelligence (AI) & It's Usages as well as the Increasing Cybersecurity & Allied Concerns have actually led to re-wiring of the minds of all the fertile, creative, innovative and humanely intelligent brains of the people of every age group especially, the youth i.e., 18-35 years of age group in such a destructive manner that every second or third person keeps on thinking as a criminal mastermind for the sake of a psychological kick from euphoria resulting from the malevolent intention of seeking revenge, satisfying the never-ending greed for easy money, for land extortion, and so on

where the humanity seems to end and the dark era of sins, greed, and all the negativity seem to begin in the very same moment at a speed which every single heart beats in the entire world.

People have become highly temperamental, sentimental, fickle-minded, crazy, maniac, impatient, unstable as well as psychologically criminogenic and almost completely devoid of humanity with the increased influence of the cyberspace and artificial intelligence in various forms like:

1. Social Media and it's addiction;
2. Screen Addiction due to abuse of Android Smartphones, Laptops, PCs, Desktops and so on;
3. Misuse as well as the Abuse of the Resourceful and enormously Infinite Cyberspace;
4. Excessive Release of Adrenaline, Dopamine, Serotonin and other Endorphins due to Excessive Usage of Social Media, OTT Platforms, and all the various forms of the infinite cyberspace as the Brain gets overloaded with the Junk Thoughts as food rather than organic, creative, natural and humanly intelligent ideas and thoughts;
5. Online Trends like Celebrating Festivals alongwith the Organizing Various Social Events as well as Corporate & Work as well as the Educational Events and other kinds of Events on Virtual Platforms like Zoom, Google Meet, Skype, and so on;
6. Enjoying Everything on the Various Kinds of Screens while depriving one's own self of nature's bounty, humanity, social connection and an art of leading a real life in a true sense as in having an innovative and a dynamic routine including family trips, casual outings, spending time with family, friends as well as all the loved ones in any possible way;
7. Cyberspace and Artificial Intelligence have created such attractive and addictive apps, softwares as well as the games that keep everyone hooked to their smartphone screen making them actually dumb, slow and devoid of common sense, locomotive senses, and all the reflexes leading to the end of true Human Intelligence Quotient (IQ).

*****

EMPOWERING ELDERLY INDIVIDUALS: THE ROLE OF DIGITAL MEDIA IN CYBERCRIME

***Naina Chudasama*[4]**

ABSTRACT

The research delves into the crucial realm of digital literacy and cybercrime awareness among older people, shedding light on their engagement with technology and susceptibility to online threats. Against the backdrop of a rapidly aging global population, where one in six individuals will be aged 60 or above by 2050, the study assumes paramount importance in addressing the evolving needs and challenges faced by elderly individuals This study delves into the awareness and literacy levels regarding digital media and cybercrimes among elderly individuals. Employing a survey methodology, data was collected from a sample of elderly respondents through a questionnaire format threw Google forms from 3 cities (namely Ahmadabad , Dhagandhra , Bhavnagar)of Gujarat which ranks 3rd in India for cyber crime and one call every 4 minute made for reporting cyber crime focusing on their digital media usage, awareness of cybercrimes, and comprehension of cyber security measures. The findings uncover a notable paradox. Despite a significant proportion of elderly individuals (66%) frequently utilizing digital platforms, particularly for financial transactions, their proficiency in digital literacy remains low, with only 6% rating themselves highly proficient. While there is a growing acknowledgment of the importance of social media (88% recognize its significance for connection and information), awareness of newer digital media formats is lacking. Of particular concern is the inadequate awareness of cybercrimes, with 40% of respondents reporting limited or no awareness, despite a considerable number falling victim to fraudulent activities. Moreover, there is a concerning lack of understanding regarding cyber security measures, with 60% unaware of concepts such as malware and cookies, and 50% lacking awareness of bank privacy policies. The study underscores the urgent need for targeted educational initiatives tailored to the elderly demographic to bridge the digital literacy gap and enable safe navigation of the digital landscape.

Keywords: Elderly population, Digital literacy ,Cybercrimes awareness, Cyber security measures and targeted educational programs.

INTRODUCTION

The research delves into the crucial realm of digital literacy and cybercrime awareness among older people, shedding light on their engagement with technology and susceptibility to online threats. Against the backdrop of a rapidly aging global population, where one in six individuals will be aged 60 or above by 2050, the study assumes paramount importance in addressing the evolving needs and challenges faced by elderly individuals (United Nations, 2020).

The central question guiding this research revolves around understanding the extent of digital literacy and cybercrime awareness among older people, given their increasing reliance on digital platforms for various activities. In light of this, the research problem centers on identifying the gaps in knowledge and awareness concerning digital media and cybersecurity measures among the elderly demographic.

The main idea of this thesis is that we need to create education and awareness programs specifically

[4] Student, UWSL , Karnavati University, India.

for the elderly to boost their digital literacy and protect them from cybercrimes. By providing them with the right knowledge and resources, we can help elderly people safely use technology and avoid online dangers.

This research is necessary because it addresses critical social challenges related to digital inclusion and cyber security for older people. By promoting cyber literacy among older individuals, we can create a more secure and equtable digital environment for everyone. Furthermore, this research is relevant to the legal landscape because it emphasizes the importance of protecting the privacy and help them live a degnified living in an increasingly digital world.

"Be prudent, be sceptical, be alert while navigating the digital world!"

THE NEED

Elderly People

"Globally 1 in 6 people in the world will be aged 60 years or over. The population aged 60 years and over will increase from 1 billion in 2020 to 1.4 billion by 2050. The number of persons aged 80 years or older is expected to triple between 2020 and 2050 to reach 426 million."

In India In the Year 2050 ,one in every five Indian will be a senior citizen. The Ministry of Social Justice and Empowerment has projected that the Indian Elder population will grow from 110 million to 320 million, which as a percentage of population is 8% to 19%. the statistical data follows similar trends. 10.7% of the total population is aged 60 and above, and the numbers are only rising. The life expectancy after the age of 60 is another 18.8 years - a clear indicator that modern medicine and facilities are now enabling people to live longer

A small percentage of the senior citizen population in India live alone (4.9%), while the majority of the elderly population live with their children (71%). 42.5% of senior citizens in India receive pensions and 23.1% are still active in the job market. 70.8% of the older population reside in rural India, with 29.2% .

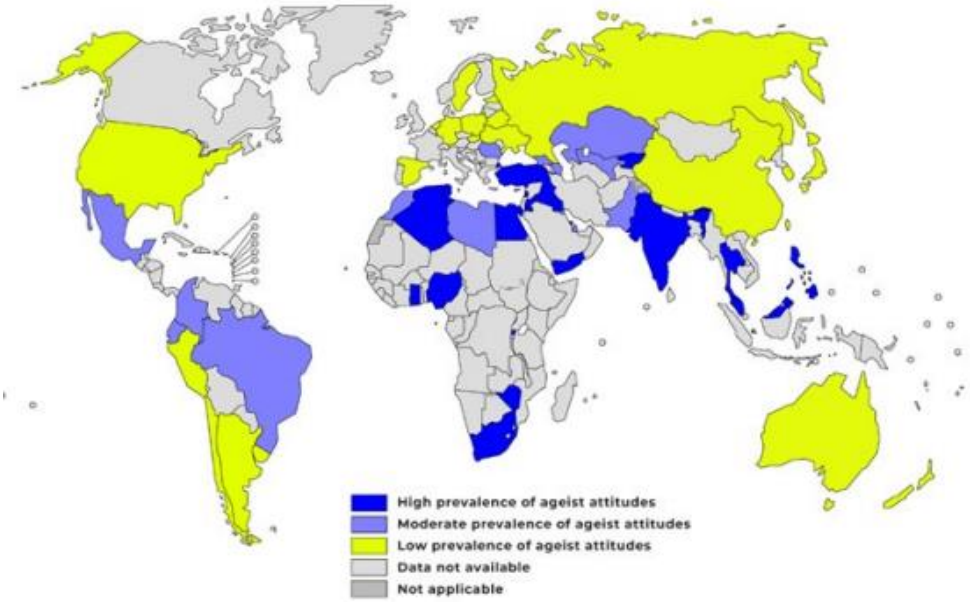
Ageing, a natural process, brings forth a host of challenges including declining physical health, shrinking social circles, and heightened feelings of loneliness, anxiety, and stress. Alterations in sleep patterns and appetite, coupled with a waning interest in daily activities, further contribute to the overall decline in both physical and mental well-being. For senior citizens, these challenges encompass both health-related issues exacerbated by age and societal discrimination based on ageism. Health ailments such as hearing loss, vision impairment, lower back pain, and falls are prevalent among the elderly, with data indicating a concerning increase in these conditions, particularly among those aged 90 and above. Concurrently, ageism persists as a pervasive issue, with a significant portion of society exhibiting discriminatory attitudes toward older individuals.

Ageism, characterized by discriminatory actions and stereotypes rooted in age, perpetuates the misconception that older individuals are inherently incapable or unsuitable for certain tasks or opportunities. This bias is detrimental not only in social settings but also in the workforce, where older

workers often face unjust treatment and economic repercussions. Contrary to stereotypes, diversity in age, like diversity in race and gender, fosters a more inclusive and productive work environment.

As longevity becomes a defining aspect of human progress, with projections indicating a substantial increase in the elderly population by 2050, it is crucial to recognize the value and potential of older individuals. Despite the prevalence of age bias fueled by capitalist and urbanized societies, addressing ageism and embracing the diverse contributions of older individuals is essential for societal advancement. Being urban dwellers.

Fig. 2.2. Map of countries showing countries classified as low, moderate or high in ageist attitudes



Digital media, transmitted through digital cables or satellites using binary signals, encompasses various forms of content like videos, articles, music, and more, accessible via devices such as computers and smartphones. It gained prominence in the latter half of the 20th century, with the internet's expansion into American households in the 1990s marking a key shift from analog to digital communication. Digital media continues to evolve rapidly, with increasing integration of AI and holographic technologies.

In India, by January 2023, there were 692 million internet users, with rural users slightly outnumbering urban ones. Internet penetration reached 48.7% of the population, and the number of users is projected to rise to 900 million by 2025. Cheaper data plans and widespread smartphone availability have driven this growth, fueling activities like online shopping and social media use, which in turn have contributed to societal and economic improvements.

Previous Study Shows the following:

As per symbiosis school findings 82% senior citizens are the users of digital devices. 75% are graduate in post graduate degree holders and 25% of school level educated. 97% users have said that they you

social media to you social media friend for friends and family and entertainment 97% users have said that they use digital devices for social media , friend and family and entertainment purposes. Out of best statistics 60% users are in aware about data mining cookies. Most of the users used bank transfer. 74% of the senior citizens with patience wait for help. 77% lle people use families help when having any problem while using the technology cal devices 10% you ask for friends help 11 to 12% ask for Google help and 1.77 people don't approach anyone. 3 in 5 seniors citizens feel independent when the use digital devices and one in three senior citizen feels relevant when the use digital devices. 69% are willing to use digital devices and digital literacy.

AGEISM – A UNSEEN BIAS

Ageing, a natural process, brings forth a host of challenges including declining physical health, shrinking social circles, and heightened feelings of loneliness, anxiety, and stress. Alterations in sleep patterns and appetite, coupled with a waning interest in daily activities, further contribute to the overall decline in both physical and mental well-being.

For senior citizens, these challenges encompass both health-related issues exacerbated by age and societal discrimination based on ageism. Health ailments such as hearing loss, vision impairment, lower back pain, and falls are prevalent among the elderly, with data indicating a concerning increase in these conditions, particularly among those aged 90 and above. Concurrently, ageism persists as a pervasive issue, with a significant portion of society exhibiting discriminatory attitudes toward older individuals.

Ageism, characterized by discriminatory actions and stereotypes rooted in age, perpetuates the misconception that older individuals are inherently incapable or unsuitable for certain tasks or opportunities. This bias is detrimental not only in social settings but also in the workforce, where older workers often face unjust treatment and economic repercussions. Contrary to stereotypes, diversity in age, like diversity in race and gender, fosters a more inclusive and productive work environment.

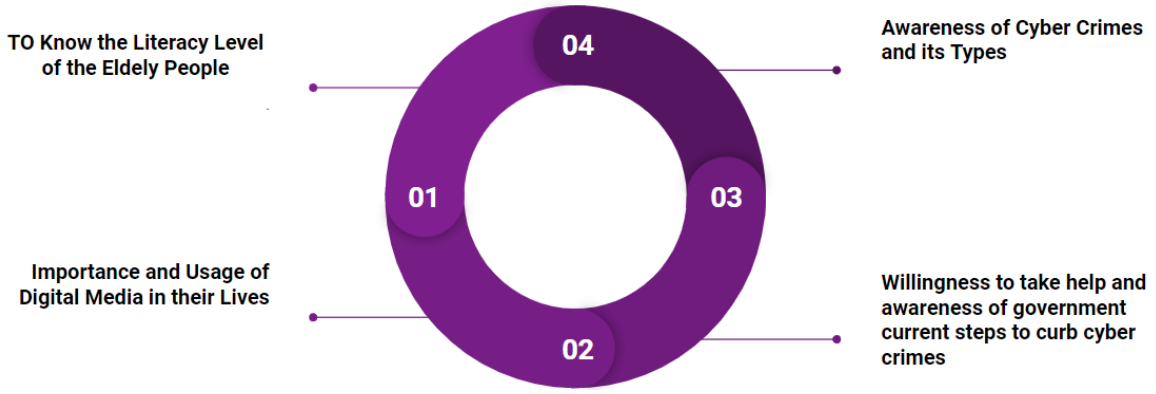
As longevity becomes a defining aspect of human progress, with projections indicating a substantial increase in the elderly population by 2050, it is crucial to recognize the value and potential of older individuals. Despite the prevalence of age bias fueled by capitalist and urbanized societies, addressing ageism and embracing the diverse contributions of older individuals is essential for societal advancement.

RESEARCH OBJECTIVES

- To understand the Digital Literacy of the elderly people
- The use of Digital Media and its other forms by them
- The awareness of Cybercrime amongst them

- The Willingness to learn Technology
- The Willingness amongst elderly people to approach the Officials for help .

KEY AREAS OF FOCUS

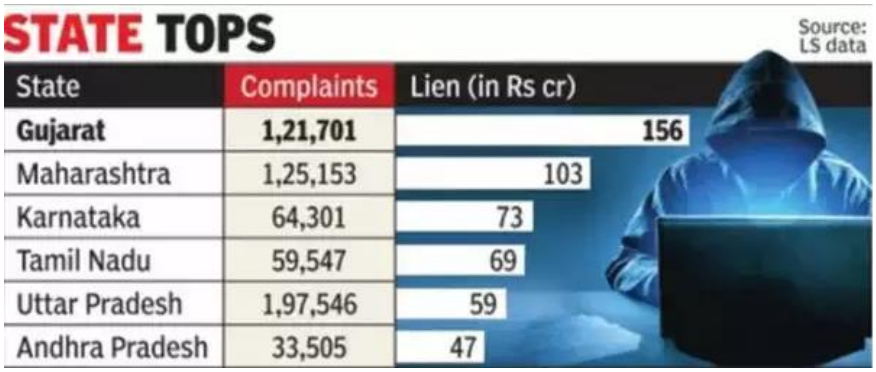


Demography

For the purpose of equal understanding of digital and Cyber crime awareness among elderly people Gujrat was Choosen By 2036, 15% of Gujarat's population will comprise elderly people. And it has 82 % population has digital literacy .A data tabled in Lok Sabha earlier this week indicated that Gujaratis lost or could not access Rs 156 crore due to financial cyber frauds in 2023. It was the highest amount frozen in cyber frauds for any Indian state -- 17% of the total amount under lien (frozen/ suspended by the bank or financial institution) across India. Gujarat died 121701 calls me to 1930 the national cyber crime helpline in 2023 making 333 calls daily or one call every 4 minute which made Gujarat rank 3 in India.

3 Areas were Choosen which provide an overview and in guiest the findings for the research objectives .

- Ahmedabad – Urban , Metropolitan City of Gujarat
- Bahnagar – It is the Developing city of Gujarat
- Dhangadhra – Taluka and Under developed area of Gujarat .



RESEARCH METHODOLOGY

The Research Methodology was Quantitative Research which consisted of primary research which

included drawing the questionnaire, piloting it and then rolling it out to the larger audience for their response. The desk research helped in identify key-areas surrounding digital literacy, Cyber crime Awareness, Ability to ask for help and usage among senior citizens. The kick-off meeting for the Research project was on 3rd April, 2024 and the outline of the objectives of the primary research was done.

The initial part focused on two main activities, developing a questionnaire to collect primary data from Senior Citizen on digital literacy via Google forms and desk research to understand more about the research topic from secondary sources like publications from government sources, newspapers, journals & international organizations

The pilot Google form was prepared and shared .The form was further tweaked to incorporate all inputs and the final questionnaire was released on 5th April, 2024.

The Google Forms questionnaire aims to assess Senior Citizens' digital literacy and awareness of cybercrime.It also aimed to understand the Knowledge of Cyber crime , their most used form of transaction and other demographic indicators.

Within 10 days the research had 50 Responses which led to the following findings .

The Research From and Findings can be Classified into 4 Parts

A. General Data of the Responders including their mode and Source of Income

B. The Awareness and Importance of Digital Media

C. The Awareness and Literacy of Cyber Crimes

D. Current preventive Measures

A. General Data of the Responders including their mode and Source of Income

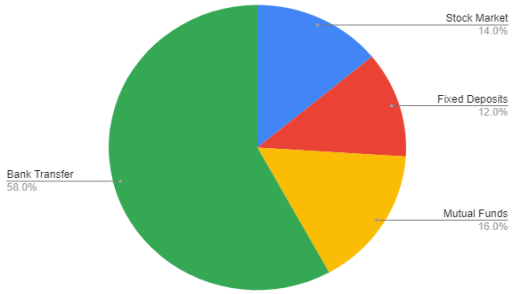
The research included responses from a gender-balanced sample, consisting of 52% males and 48% females, with a total of 50 participants. According to the National Elderly Policy, individuals aged 60 and above are classified as elderly, and thus, the minimum age in the study was set at 60 years.

The age distribution of participants is as follows:

No.	Age	Ratio
1	60-70	48%
2	70-80	28%
3	80-90	20%
4	90 & Above	4 %

Regarding sources of income, 30% of respondents rely on pensions, and another 30% derive income from interest. Dividends account for 14% of income, while 16% of participants are still employed. Additionally, 2% earn through freelancing or consulting, and 8% reported being unemployed. This

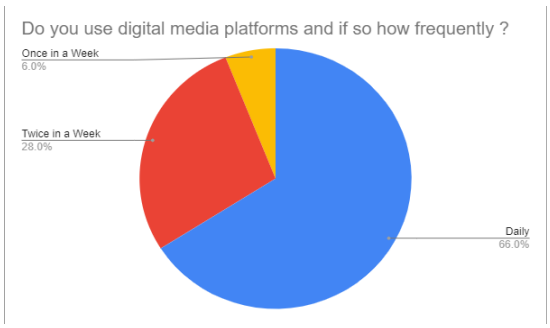
detailed breakdown offers insights into the financial dynamics of the elderly population included in the study.

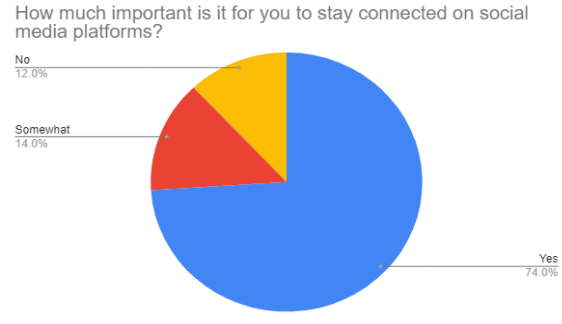


B. The Awareness and Importance of Digital Media

Elderly individuals show a clear preference for certain financial transaction methods, with 58% primarily using bank transfers. Other methods include mutual funds, which account for 16%of their transactions, followed by 14% in the stock market, and 12% in fixed deposits. This reflects a cautious yet balanced approach to financial management, with a focus on stability and moderate risk.

In terms of digital media usage, a significant 66% of elderly participants access digital platforms daily, while 28% engage with these platforms twice a week, and 6% use them once a week. This indicates a growing reliance on digital tools for various activities, highlighting the increasing integration of technology into their daily lives. However, when it comes to digital literacy, the responses show a broad spectrum. While 54% of the elderly consider their digital literacy to be average, only 12% rated themselves as having good digital skills. On the other hand, 28%of respondents reported having very poor digital literacy, and just 6% felt they were highly proficient in using digital platforms. This disparity points to the varying levels of comfort and competence with technology among the elderly population.





When assessing their ability to use digital newspapers, the proficiency gap becomes more evident. Only 10%of the elderly reported being proficient in this area, while 32% felt somewhat competent. A small percentage, 6%, were unsure about their abilities. However, the majority—52%—admitted to having no digital literacy related to newspapers. This highlights a significant gap in their ability to access and engage with news through digital platforms, underscoring the need for targeted efforts to improve their digital media skills.

C. The Awareness and Literacy of Cyber Crimes

Cyber Fraud Awareness and Experiences Among the Elderly

A significant portion of elderly individuals, either personally or through family members, have experienced cyber fraud, with 48%of respondents reporting such incidents, while 52%indicated they had not encountered any form of cyber fraud. This highlights the growing vulnerability of the elderly population to online threats.

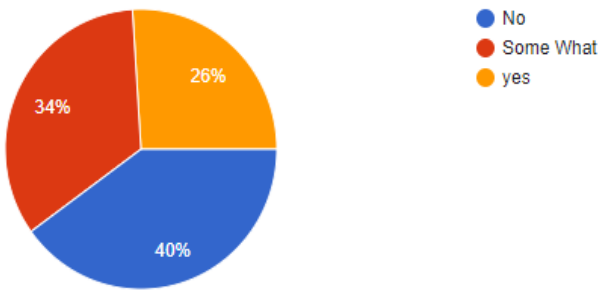
When it comes to their awareness of cyber fraud, the responses show varied levels of understanding. Only 26% of elderly participants are fully aware of cyber fraud risks, while 34% possess partial awareness. However, a concerning 40% of respondents admitted to having no awareness at all, emphasizing the need for greater education and protection against online scams.

Similarly, the elderly demonstrate limited knowledge about malware and cookies, two common elements in online security breaches. And merely 12% of respondents reported being aware of these threats, with 28% somewhat familiar with them. Alarmingly, 60% of the participants had no awareness of malware and cookies, underscoring their exposure to potential cyber risks.

Further concerns arise regarding the elderly's understanding of banks' privacy conditions, an essential aspect of protecting financial information online. None of the participants 0% were fully aware of these privacy terms, while 8%had a partial understanding. A significant 42%were uncertain about these conditions, and 50%admitted to having no awareness. This gap in knowledge could make them more susceptible to fraud in financial transactions.

The emotional impact of cyber fraud is also notable. 20% of elderly victims reported feeling ashamedof being defrauded online, while 38% were unsure of their feelings, and 42%stated they did not feel ashamed. Furthermore, when asked about self-blame, 52% of respondents admitted to blaming themselves for falling victim to cyber fraud, while 48% did not attribute the fault to themselves. This suggests that beyond financial loss, cyber fraud also takes an emotional toll on the elderly, affecting their sense of confidence and security online.

These findings highlight the urgent need for targeted initiatives to raise awareness about cyber fraud and enhance the digital literacy of elderly individuals, thereby equipping them to navigate the digital world more safely and confidently.



D. Current preventive Measures

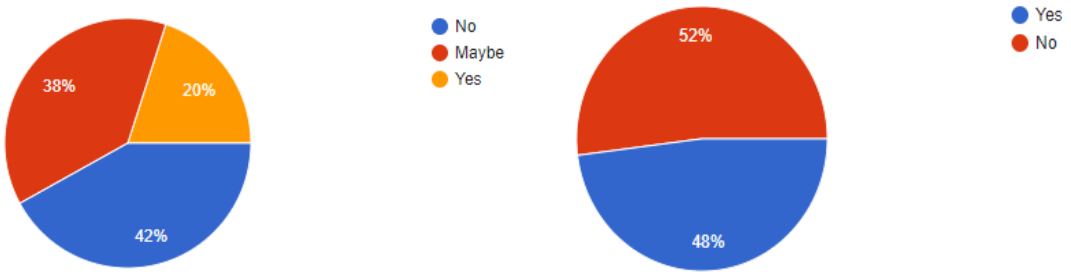
Elderly individuals exhibit a notable willingness to seek assistance from government and police services in case of cyber issues, with 72% expressing readiness to approach these authorities. However, 18% remain uncertain about seeking help, and 10% would not consider reaching out for assistance. This indicates a generally positive attitude towards involving official channels for support, but a small portion still hesitates to do so.

When it comes to awareness of specific resources, 56%of the elderly are aware of the cyber cell within the police force, a key resource for addressing cybercrime. On the other hand, 44% are unfamiliar with this service, reflecting a gap in knowledge that could hinder timely reporting and intervention in cyber fraud cases.

Awareness initiatives conducted by banks to educate elderly individuals about cyber safety have yielded mixed results. 44% of respondents are aware of these initiatives, with 10% being aware but choosing not to engage with them. Unfortunately, a significant 46%have no awareness of such efforts. This suggests that, while some outreach is effective, there is still a large portion of the elderly population that remains uninformed, making them more vulnerable to online threats.

Moreover, community discussions on cyber security are strikingly low. Only 2%of elderly individuals actively engage in conversations about cyber safety, while 22%are aware of such discussions but do not participate. A substantial 76% have never engaged in any discussions related to cyber security, highlighting a major disconnect in communal efforts to address and share knowledge about online safety. This lack of engagement underscores the need for better community-based initiatives to raise awareness and encourage dialogue among the elderly about the importance of cyber security.

These findings reveal both the willingness and gaps among elderly individuals in seeking help and participating in cyber security education. More focused outreach efforts and increased community engagement are essential to ensure that this vulnerable demographic is better equipped to handle the challenges of the digital world.



ANALYSIS

Digital Literacy and Cybercrime Awareness Among the Elderly Population

The research findings on the digital media usage, literacy, and awareness of cybercrimes among elderly individuals offer crucial insights into their interaction with technology and their vulnerability to online

risks. As the digital landscape continues to expand, understanding how elderly individuals engage with these technologies, their awareness levels, and the challenges they face becomes vital for developing targeted strategies to protect them from cybercrime. This analysis highlights the key findings from the study, focusing on the financial independence of the elderly, their usage of digital platforms, and the gaps in cybercrime awareness.

Age and Income Diversity

The research encompasses a wide range of elderly individuals, predominantly within the 60–70 age bracket, aligning with the definition of elderly according to the National Elderly Policy. This diverse age distribution provides a comprehensive view of how different segments of the elderly population interact with technology. Financial independence emerges as a significant theme in the study, with pension and interest income being the two primary sources of income for 60% of the respondents. This indicates a degree of financial security among elderly individuals, making them active participants in financial transactions, often conducted digitally.

Despite this financial independence, many elderly people remain vulnerable to cyber threats, given their regular engagement with online banking and other financial platforms. This connection between financial independence and the use of digital platforms underscores the need for heightened awareness and education on cyber threats that target financial activities.

Digital Media Usage and Literacy

The research reveals a relatively high rate of digital media usage among the elderly. 66% of respondents reported using digital platforms daily, particularly for financial transactions such as bank transfers , which account for 58% of their online activities. This indicates that a significant portion of the elderly population is reliant on digital platforms to manage their finances, reflecting a growing trend of elderly individuals embracing technology for essential activities. Additionally, 16% of respondents prefer using digital platforms for mutual funds , followed by 14% for stock market transactions, further demonstrating the role of digital media in their financial management.

However, while the usage of digital platforms is high, the overall digital literacy among the elderly remains a concern. Only 6% of respondents rated their digital literacy as "very high," indicating that despite frequent use, most elderly individuals struggle with navigating digital platforms. 54% of the elderly rated their digital literacy as average, while 28% considered their skills to be very poor. This disparity between usage and proficiency points to a crucial gap that needs to be addressed.

The research also shows a growing recognition of the importance of social media, with 88% of respondents acknowledging its relevance for staying connected. However, despite this awareness, there is a lack of understanding of newer forms of digital media, such as digital newspapers, with only 10% of respondents feeling proficient in accessing news digitally. This gap highlights that while elderly individuals may use technology for specific purposes, their knowledge of other useful digital resources is limited.

Cybercrime Awareness and Vulnerability

The most alarming findings from the research relate to the elderly's awareness of cybercrime and their vulnerability to online threats. While 26% of respondents demonstrated some level of awareness about cyber fraud targeting the elderly, a staggering 40% admitted to having limited or no knowledge of such threats. Despite 48% of respondents or their family members having been victims of cyber fraud, the lack of awareness regarding the risks of cybercrime is significant. Moreover, many elderly individuals tend to blame themselves for falling victim to online scams, with 52% expressing feelings of self-blame. This emotional toll, coupled with the lack of awareness, indicates a deep-seated issue that needs to be addressed through education and support mechanisms.

Awareness of cyber security measures is also worryingly low. 60% of respondents were unaware of basic online security concepts such as malware and cookies, essential tools for safeguarding against cyber threats. Similarly, only 8% of respondents had any awareness of bank privacy policies, and 50% admitted to being completely unaware of these crucial terms. This lack of knowledge leaves elderly individuals particularly susceptible to various forms of cybercrime, including credit card fraud and internet banking scams.

Preventive Measures and Community Engagement

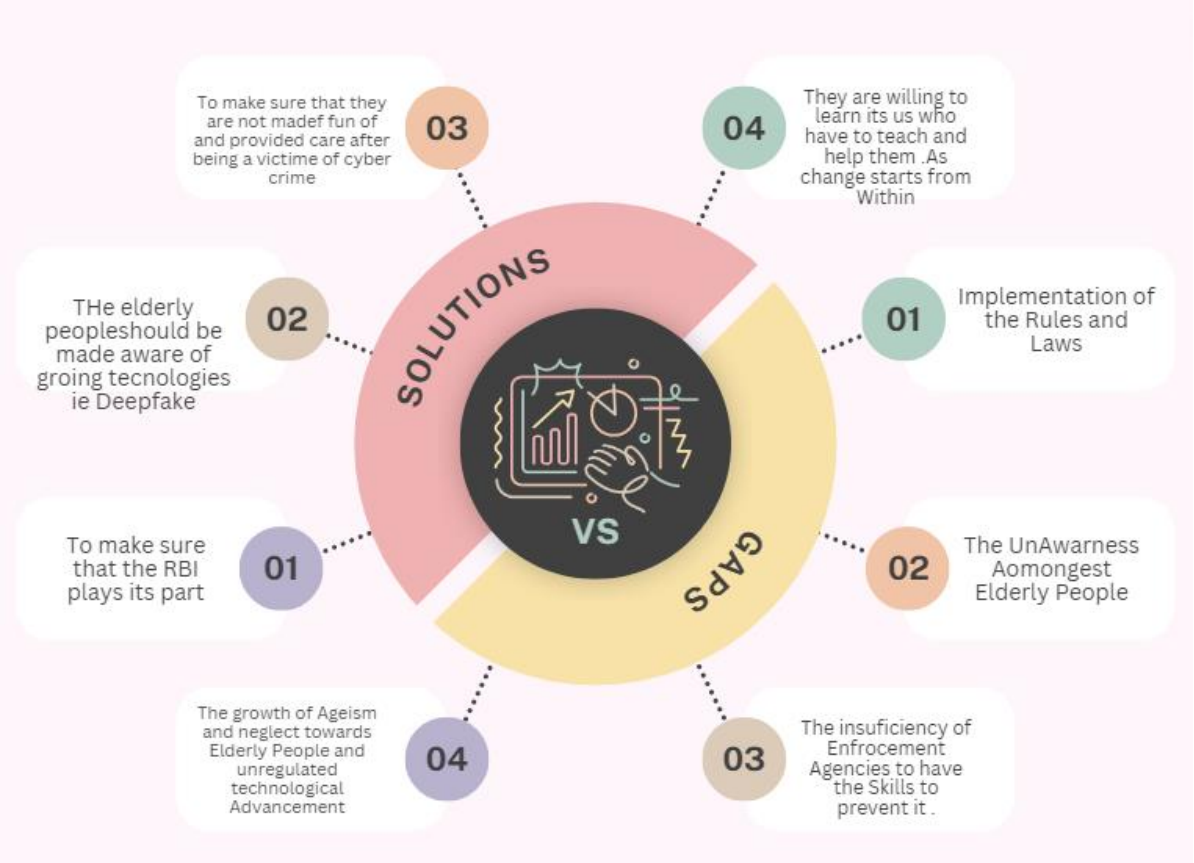
While the research shows some awareness of preventive measures, particularly from banks' initiatives aimed at educating elderly individuals about cyber threats, engagement with these initiatives remains limited. 44% of respondents were aware of such programs, yet many do not actively participate or utilize them. Moreover, community discussions about cyber security are minimal, with only 2% of respondents actively engaging in these conversations. 76% reported never discussing cyber security, further highlighting the isolation of elderly individuals from critical conversations about online safety. This lack of communal support exacerbates their vulnerability, as many elderly individuals may not know where to turn for help or advice when faced with online threats.

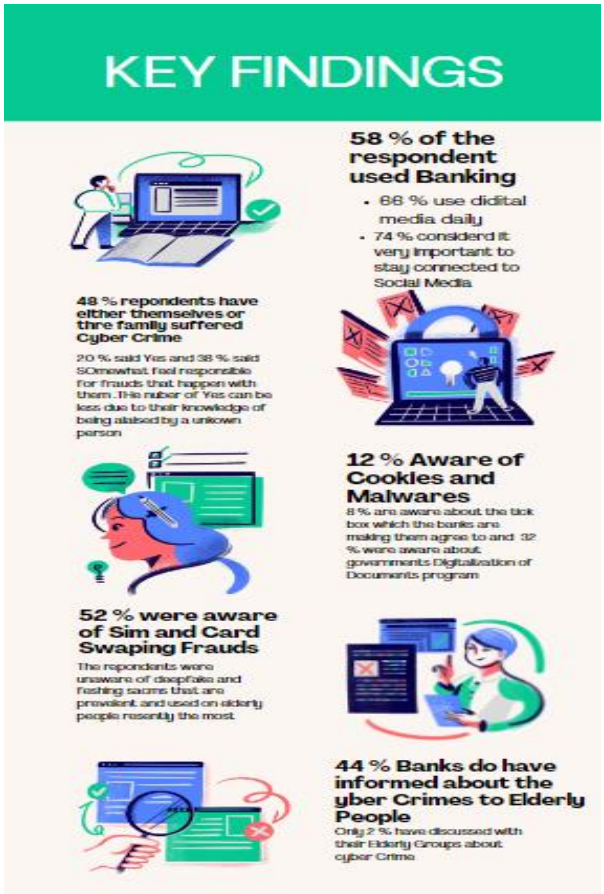
RESENT STEPS BY GOVERNMENT AND COURTS

Kerala Government has decided to amend the Police Act to include intimidation, defamation, or insulting of any person through social media as an offence punishable with imprisonment of term upto five years and/or upto 10,000/- fine. The Kerala Cabinet has also decided to recommend to the Governor to promulgate an ordinance in this regard. A new Section 118A will be added to the Kerala police Act.

The Madras High Court on Thursday allowed Internet Freedom Foundation(IFF) to intervene in the petitions which seek directions to link Aadhaar with social media accounts.The IFF opposes interlinking of Aadhaar and social media profiles on the ground that it will result in vesting unbridled power on social media companies over the lives of users, resulting in infringement of privacy. Antony Clement Rubin v. Union of India & Ors (W.P. No. 20774/2018)and Janani Krishnamurthy v. Union of India (W.P. No. 20214/2018).

THE WAY FORWARD


SOLUTIONS
VS
GAPS
03
To make sure that they are not madef fun of and provided care after being a victime of cyber crime
04
They are willing to learn its us who have to teach and help them .As change starts from Within
02
THe elderly peopleshould be made aware of groing tecnologies ie Deepfake
01
Implementation of the Rules and Laws
01
To make sure that the RBI plays its part
02
The UnAwarness Aomongest Elderly People
04
The growth of Ageism and neglect towards Elderly People and unregulated technological Advancement
03
The insuficiency of Enfrocement Agencies to have the Skills to prevent it .


KEY FINDINGS
58 % of the respondent used Banking
88 % use didital media daily
74 % considerd it very important to stay connected to Social Media
48 % repondents have either themselves or thre family suffered Cyber Crime
20 % said Yes and 38 % said SOmewhat feel responsible for frauds that happen with them .The nuber of Yes can be less due to their knowledge of being abused by a unkown person
12 % Aware of Cookies and Malwares
8 % are aware about the tick box which the banks are making them agree to and 32 % were aware about governments Digitalisation of Documents program
52 % were aware of Sim and Card Swaping Frauds
The repondents were unaware of deepfake and fishing sacms that are prevalent and used on elderly people resently the most
44 % Banks do have informed about the yber Crimes to Elderly People
Only 2 % have discussed with their Elderly Groups about cyber Crime

CONCLUSION

The research highlights a clear digital divide among the elderly. While many seniors engage with digital platforms daily, especially for financial activities, their overall digital literacy remains low, with only 6% rating themselves highly proficient. Despite recognizing the importance of social media (with 88% acknowledging its significance), their knowledge of newer forms of digital media, such as e-papers, remains limited.

More concerning is the lack of awareness around cybercrime, with 40% of elderly respondents having limited or no knowledge of online threats, despite many falling victim to fraud. The understanding of essential cybersecurity measures, such as malware and cookies, is also lacking, with 60% unaware of these risks. Additionally, 50% are unfamiliar with their banks' privacy policies, further exposing them to vulnerabilities in financial transactions.

These findings emphasize an urgent need for tailored educational programs focused on improving the digital literacy of seniors. Such programs should equip them with the necessary skills to safely navigate digital platforms, protect their personal information, and reduce their risk of cybercrime. By addressing these gaps, elderly individuals can fully benefit from technology while safeguarding themselves from online threats.

*****

CROSS-BORDER CYBERCRIME IN THE METAVERSE: NAVIGATING JURISDICTIONAL CHALLENGES AND LEGAL GAPS

Khandokar Al Wasi[5]

ABSTRACT

The metaverse, a virtual space where users interact through digital avatars, presents new challenges in addressing cross-border cybercrime. The paper explores the legal and jurisdictional gaps in this borderless virtual space, where cybercriminals exploit vulnerabilities and traditional legal frameworks struggle to enforce regulations. The urgent need for international cooperation and legal reform is highlighted, with the Draft United Nations Convention Against Cybercrime assessing its potential to standardize global responses to cyber threats. The paper also discusses the challenges of establishing jurisdiction in the metaverse, particularly with the rise of decentralized technologies and virtual currencies. The paper proposes international agreements and adaptable legal standards to address these gaps. The paper also discusses the role of artificial intelligence in combating cybercrime, emphasizing its potential but also raising ethical concerns.

INTRODUCTION

The metaverse represents a rapidly growing virtual environment where individuals interact, socialize, and engage in commercial activities through digital avatars. This expansive digital space encompasses a network of 3D virtual worlds, facilitated by virtual reality (VR), augmented reality (AR), and other immersive technologies, offering users a blend of social interaction, entertainment, and economic transactions. However, with this immense potential for innovation comes significant risk, particularly in the realm of cybercrime. The borderless nature of the metaverse introduces complexities in legal jurisdiction, making it challenging to regulate and prosecute cybercriminal activities that span multiple countries. Traditional legal frameworks, designed for the physical world or early internet structures, are increasingly inadequate for addressing crimes committed in this decentralized, virtual space.

The growth of the metaverse has made it a prime target for cybercriminals who exploit the anonymity and transnational nature of the platform. For example, crimes such as identity theft, financial fraud, and intellectual property violations are prevalent in the metaverse, raising significant concerns about jurisdictional enforcement and accountability. With users from different countries engaging simultaneously in virtual environments, the question of which nation has the authority to enforce laws becomes increasingly complex. The transnational nature of the metaverse creates jurisdictional gaps that cybercriminals exploit, allowing them to commit offenses in one country while residing in another, often using decentralized technologies like blockchain and cryptocurrencies to further obscure their identities and activities. These factors highlight the urgent need for international cooperation and reform in legal frameworks to effectively address cross-border cybercrime in this new digital era.

This paper aims to investigate the legal and jurisdictional challenges surrounding cross-border cybercrime in the metaverse, with a particular focus on how current legal frameworks are ill-equipped to deal with these issues. Central to this discussion is the analysis of the Draft United Nations

[5] Student at American International University, Bangladesh.

Convention Against Cybercrime, which seeks to standardize international responses to cyber threats. The research will explore specific case studies to illustrate the challenges law enforcement agencies face in identifying and prosecuting cybercriminals in the metaverse. Moreover, it will assess how traditional concepts of jurisdiction are challenged by the fluid and decentralized nature of this virtual environment and propose legal reforms that could close these gaps. Additionally, this paper will delve into the role of artificial intelligence (AI) in assisting law enforcement and the ethical concerns that arise in its application, such as balancing privacy rights with the need for security.

Ultimately, this research argues for the urgent reassessment of existing legal frameworks and stronger international collaboration to effectively combat cross-border cybercrime in the metaverse. By addressing jurisdictional challenges and fostering cooperation among nations, the global community can work towards creating a safer virtual environment for all users.

LITERATURE REVIEW

Cybercrime in Traditional Digital Spaces

Cybercrime, defined broadly as criminal activities conducted through digital means, has evolved significantly since the advent of the internet. Early cybercrimes were often limited to offenses such as hacking, phishing, and identity theft, but as technology advanced, so too did the nature and complexity of cyber offenses. Cross-border cybercrime has posed significant challenges to legal and enforcement agencies, given that cybercriminals can exploit the jurisdictional boundaries of different countries to evade prosecution. In traditional digital spaces—often referred to as cyberspace—the global nature of the internet has facilitated criminal activities that transcend national borders, creating complications for law enforcement and judiciary systems.

Research on cross-border cybercrime in traditional digital spaces has primarily focused on issues such as data privacy, intellectual property theft, and financial fraud. Scholars like Brenner (2006) have highlighted the jurisdictional complexities involved in prosecuting cybercrimes, noting that countries have different legal definitions of what constitutes a cyber offense and varying levels of law enforcement capabilities. Another critical issue identified in the literature is the attribution problem, where it is difficult to trace and identify the perpetrators of cybercrimes due to the anonymity offered by digital technologies. This anonymity, coupled with the ease of committing offenses from remote locations, allows criminals to operate with a reduced risk of being caught.

International cooperation has been a central theme in addressing these challenges. One of the most significant initiatives in this space has been the Budapest Convention on Cybercrime, which serves as the first international treaty seeking to harmonize cybercrime laws and foster cooperation among nations. While the Budapest Convention has achieved some success, its effectiveness has been hampered by the lack of global participation and the varying degrees of its implementation across jurisdictions. As traditional cyberspace continues to evolve, these challenges persist, but new digital environments like the metaverse add further layers of complexity to the existing frameworks.

Emergence of the Metaverse and New Legal Complexities

The rise of the metaverse—a collective virtual shared space that blends virtual reality (VR), augmented reality (AR), and other immersive technologies—has introduced new dimensions to the conversation on cybercrime. Unlike traditional online environments where interactions are primarily two-dimensional, the metaverse offers an immersive experience where users can engage in real-time interactions through avatars. While this presents opportunities for social, economic, and creative ventures, it also opens up avenues for criminal activities that are more sophisticated than those in traditional cyberspace.

Cybercrime in the metaverse introduces new legal complexities. Due to the immersive nature of the metaverse, cyber offenses in this space can range from virtual identity theft to avatar-based harassment, virtual property theft, and even financial crimes conducted through decentralized virtual currencies like cryptocurrency. Moreover, the decentralized nature of many metaverse platforms makes it difficult to establish legal jurisdiction, as the platforms may be operated by entities spread across multiple countries.

The academic literature has begun to address these issues, with scholars like González and Castejón (2022) emphasizing the jurisdictional challenges posed by the metaverse. They argue that while cybercrimes in traditional digital spaces may be prosecuted under existing frameworks, the virtual and decentralized nature of the metaverse blurs the lines between real-world and virtual-world interactions. As a result, current laws may be insufficient to protect users from offenses in the metaverse, requiring new legal definitions and frameworks to effectively regulate and enforce laws in this space.

International Legal Frameworks and Jurisdictional Challenges

Addressing cross-border cybercrime requires international cooperation, but the existing legal frameworks, such as the Budapest Convention on Cybercrime, face challenges when applied to the metaverse. The Budapest Convention, adopted in 2001, was designed to combat cybercrime through a comprehensive framework that fosters international collaboration and mutual assistance in investigations and prosecutions. While the convention has been pivotal in facilitating cooperation between countries, its provisions are largely focused on traditional forms of cybercrime like hacking and online fraud, which may not be fully applicable in the context of the metaverse.

Moreover, the jurisdictional challenges that have long plagued cybercrime enforcement are exacerbated in the metaverse. In traditional cyberspace, the issue of jurisdiction is already complex, as cybercriminals can operate from a different country than the victim, making it difficult to determine which nation's laws should apply. In the metaverse, this challenge is amplified by the decentralized and borderless nature of virtual worlds, where users from various countries can interact simultaneously. As Mann and Weisberg (2019) point out, the problem of jurisdiction becomes particularly pronounced when considering decentralized technologies like blockchain, which are often employed in metaverse environments. Blockchain’s anonymity and lack of a central authority make it difficult to regulate and attribute responsibility for criminal activities.

To address these gaps, scholars have called for a reassessment of current international frameworks and the development of new global agreements that take into account the unique aspects of the metaverse. Zittrain (2018) proposes a more adaptable legal approach that evolves alongside technological advancements, ensuring that legal standards remain relevant in new digital spaces. Other recommendations include the creation of specialized cybercrime task forces that operate across borders, similar to initiatives seen with international bodies like Interpol and Europol, to address the fluid nature of crime in the metaverse.

METHODOLOGY OF THE STUDY

This research adopts a qualitative approach to explore the complex dimensions of navigating jurisdictional challenges in cross-border cybercrime and the legal gaps within the metaverse. The study is grounded in both primary and secondary sources. Primary sources, including legislation and case law, form the core legal frameworks under scrutiny. Secondary sources, such as academic publications, journal articles, books, online resources, organizational reports, and media analyses, provide critical insights that complement and expand the examination of the metaverse's emerging legal landscape.

ANALYSIS OF THE DRAFT UNITED NATIONS CONVENTION AGAINST CYBERCRIME

The Draft Convention

The Draft United Nations Convention Against Cybercrime is a significant step toward creating a unified global response to the rising threat of cybercrime. Aimed at fostering international cooperation, the convention seeks to standardize legal frameworks, harmonize national laws, and enhance cross-border collaboration between nations in combating cyber-related offenses. Its overarching goals include promoting information sharing, capacity building, and legal assistance in investigations that span multiple jurisdictions, while respecting state sovereignty and fundamental human rights.

The convention emphasizes several core principles:

- **Criminalization of Cyber Offenses:** It establishes a broad array of cybercrimes, ranging from illegal access to data and system interference to more sophisticated offenses like cyber-terrorism and virtual financial fraud.
- **International Cooperation:** Recognizing the borderless nature of the internet, the draft focuses on mechanisms for real-time collaboration among law enforcement agencies globally, including sharing evidence, investigating cyber incidents, and prosecuting offenders.
- **Protection of Human Rights and Privacy:** A balance between law enforcement's need to combat cybercrime and individuals' rights to privacy is embedded in the draft convention, though achieving this balance is often contentious in practice.

While the Draft Convention is an important milestone, it faces significant challenges in addressing cybercrime within evolving digital ecosystems like the metaverse. The virtual nature of the metaverse adds layers of complexity to issues of sovereignty, jurisdiction, and law enforcement, which the convention must address if it is to be effective.

Assessing Jurisdictional Adequacy

Jurisdiction is central to the convention, as cybercrime frequently involves actors and infrastructure spread across various nations. The Draft Convention stipulates provisions for extraterritorial jurisdiction, allowing countries to claim authority in prosecuting offenders if the crime impacts their territory or citizens. However, the metaverse, with its decentralized structure and real-time cross-border interactions, creates unique challenges for enforcing such jurisdictional claims.

- **Territorial Jurisdiction:** The convention relies on the traditional concept of territorial jurisdiction, where states exercise authority over crimes committed within their borders. However, the metaverse transcends these physical borders, leading to ambiguity about where a crime occurs and which state has the legal right to prosecute. For example, if a financial fraud or identity theft occurs in a virtual world where participants from multiple countries are involved, determining the "territory" becomes difficult.
- **Personal Jurisdiction:** The convention includes provisions for personal jurisdiction, where a state can prosecute individuals if they are citizens or residents of the prosecuting nation[7]. While this may work in traditional cybercrime, the anonymity of the metaverse complicates identification, making it difficult to apply personal jurisdiction without clearer rules for tracking and identifying virtual actors.
- **Universal Jurisdiction:** In some cases, the convention allows for universal jurisdiction, particularly for crimes considered a threat to international security, such as cyber-terrorism. However, applying universal jurisdiction to the metaverse, especially for non-violent cybercrimes, remains problematic, as different states have varying thresholds for what constitutes a global threat.

Legal Gaps and Shortcomings

While the Draft Convention lays the foundation for cross-border cooperation, it lacks the specificity

needed to address the metaverse's unique legal challenges. Several gaps in the convention's framework are particularly relevant in this context:

- **Anonymity and Decentralization:** The convention does not adequately address the decentralized nature of the metaverse. Unlike traditional cyberspace, where data and communications are often stored on servers located within a specific jurisdiction, the metaverse operates on blockchain technologies and distributed networks. This decentralized architecture makes it harder to pinpoint the origin of criminal activities, which in turn complicates enforcement.
- **Virtual Identity and Property Crimes:** The metaverse introduces novel forms of criminal activity, including virtual identity theft and theft of virtual assets like non-fungible tokens (NFTs) or cryptocurrency. While the Draft Convention recognizes cybercrime in general terms, it lacks provisions specific to these types of offenses, leaving a gap in legal definitions and the scope of prosecution.

- **International Coordination and Enforcement:** Although the convention advocates for international cooperation, it fails to provide clear procedural guidelines for handling crimes committed in virtual environments that have no clear national boundaries. The absence of a multilateral enforcement mechanism specific to the metaverse could leave countries unprepared to respond effectively to such crimes.
- **Dynamic Nature of the Metaverse:** The rapid evolution of technology and the metaverse environment demands a legal framework that can adapt quickly to new challenges. However, the Draft Convention lacks mechanisms for continuous updates or the inclusion of emerging cybercrime trends, which could make it obsolete in dealing with future threats in virtual worlds.

While the Draft United Nations Convention Against Cybercrime is a significant step toward global cooperation, it remains limited in addressing the complexities of jurisdiction in the metaverse. The borderless, decentralized, and anonymous nature of the metaverse creates challenges that the convention's current provisions do not fully address. To combat cross-border cybercrime effectively in this evolving digital environment, the convention will require updates and revisions that account for the unique legal and jurisdictional issues presented by the metaverse.

JURISDICTIONAL CHALLENGES IN THE METAVERSE

Traditional Jurisdiction vs. Metaverse Jurisdiction

Traditional concepts of jurisdiction—territorial, extraterritorial, and universal—are foundational to legal systems across the world. However, these concepts face considerable challenges when applied to the metaverse, a decentralized and borderless virtual environment.

Territorial jurisdiction, the most common form of legal authority, is based on the physical location where a crime occurs. In the metaverse, this is problematic since interactions and transactions occur in a virtual space that lacks clear geographical boundaries. For example, a user in one country may commit an illegal act against another user located in a different country, but the "location" of the offense is difficult to define due to the virtual nature of the platform.

Extraterritorial jurisdiction allows a state to claim legal authority over actions that occur outside its borders if they impact national interests or citizens. In the metaverse, this jurisdictional concept struggles, particularly when determining which country's laws should apply to a crime involving multiple users from various jurisdictions, each subject to different legal systems.

Universal jurisdiction, often applied to serious international crimes like piracy or genocide, allows states to prosecute offenses regardless of where they occur. However, applying universal jurisdiction to metaverse crimes is not straightforward. Determining the severity of virtual crimes and gaining international consensus on their prosecution remains a challenge.

In summary, traditional jurisdictional principles do not easily adapt to the metaverse, where geographical boundaries blur, making it difficult for legal authorities to assert control.

Extraterritorial Jurisdiction and Double Criminality

The principle of extraterritorial jurisdiction often intersects with double criminality, a legal standard requiring that an act must be considered a crime in both the prosecuting country and the country where the crime occurred. In metaverse crimes, this principle becomes particularly challenging when countries have differing legal definitions of offenses.

For example, cyber harassment might be a serious offense in one country but not recognized as a crime in another. This leads to issues when prosecuting an individual in the metaverse, as conflicting legal standards between jurisdictions hinder extradition or prosecution. A hypothetical case could involve a user who harasses another through virtual means in the metaverse. If the harasser resides in a country that does not recognize virtual harassment as a crime, prosecuting them under extraterritorial jurisdiction becomes difficult.

Similarly, double criminality is complicated when considering financial crimes in the metaverse, particularly with the use of virtual currencies. Some countries may not have developed comprehensive legal frameworks to address crimes involving cryptocurrencies or blockchain transactions, further hindering prosecution across borders.

CHALLENGES OF VIRTUAL PROPERTY AND IDENTITY THEFT

The issue of virtual property and identity theft in the metaverse creates unique jurisdictional challenges. Crimes involving the theft of virtual assets, such as non-fungible tokens (NFTs) or virtual real estate, present new legal questions regarding ownership and territoriality. Unlike traditional property, virtual assets do not exist within physical borders, making it difficult to determine which country's laws apply.

A hypothetical case study could involve the theft of an expensive NFT within the metaverse. If the theft involves users from multiple jurisdictions, it becomes unclear which country holds jurisdiction over the crime. Additionally, the lack of legal recognition of virtual property in some countries further complicates prosecution.

Identity theft in the metaverse presents similar issues. A criminal could create a digital avatar that mimics another user's identity, using it to defraud others. Traditional jurisdictional principles struggle to address this form of theft, as the crime exists solely within the digital world, making it hard to establish a "location" for the crime. Furthermore, the anonymity of metaverse users often hinders the ability of law enforcement to identify and prosecute offenders.

The Role of Virtual Currencies

The use of decentralized digital currencies in the metaverse introduces additional jurisdictional challenges, particularly in prosecuting financial crimes. Unlike traditional currencies, cryptocurrencies like Bitcoin and Ethereum operate on decentralized networks, meaning no single country has control or oversight over transactions made in these currencies.

For instance, money laundering schemes using virtual currencies in the metaverse are difficult to trace, and prosecuting offenders is complicated by the lack of a centralized authority. The decentralized nature of these currencies allows criminals to conduct cross-border transactions that evade regulatory oversight, making it challenging for any single jurisdiction to prosecute offenders.

In addition, countries have different legal approaches to virtual currencies. Some nations heavily regulate their use, while others provide little or no regulation, creating conflicting legal standards that hinder international cooperation in metaverse-related financial crimes. This lack of uniformity in how digital currencies are treated exacerbates jurisdictional challenges, making it difficult for countries to establish a clear legal framework for addressing these offenses.

The jurisdictional challenges posed by the metaverse are vast, with traditional legal concepts struggling to adapt to this new digital frontier. Whether dealing with virtual property theft, identity fraud, or crimes involving decentralized currencies, the fluid and borderless nature of the metaverse complicates efforts to establish legal jurisdiction and prosecute offenders. Addressing these challenges will require substantial international cooperation and the development of new legal frameworks tailored to the metaverse's unique characteristics.

INTERNATIONAL COOPERATION AND ENFORCEMENT

Current Mechanisms of International Cooperation

International frameworks like Mutual Legal Assistance Treaties (MLATs) serve as critical mechanisms for addressing cross-border cybercrime, allowing countries to collaborate on investigations and prosecutions. These treaties are essential for gathering evidence and enforcing laws that transcend national borders, but they often face bureaucratic delays and inconsistent cooperation, hampering their effectiveness.

The Budapest Convention on Cybercrime is one such framework designed to facilitate international cooperation. It is the first international treaty seeking to address internet and computer crime, with a primary focus on cyber threats and cross-border crime. However, the convention has limitations, including its non-universal adoption, leaving gaps where non-signatory nations do not have a legal framework for international cooperation. Furthermore, its focus on traditional cybercrime makes it ill-equipped to address challenges posed by emerging digital spaces like the metaverse.

Other initiatives, like Interpol's Global Complex for Innovation, aim to foster cross-border cooperation by providing a platform for sharing resources and best practices. However, despite such efforts, the lack of globally consistent regulations leaves room for cybercriminals to operate with relative impunity in some regions.

Enforcement Gaps in the Metaverse

Law enforcement agencies face significant challenges when addressing crimes within the metaverse, particularly due to the borderless nature of virtual environments. A key obstacle is the lack of technological expertise among law enforcement personnel. Crimes involving blockchain technology, decentralized platforms, and virtual currencies are often beyond the capability of traditional enforcement mechanisms.

Moreover, regulatory frameworks tailored to traditional cybercrime are not equipped to handle the dynamic, fluid nature of crimes committed within the metaverse, where jurisdictional boundaries

become blurred. Crimes such as virtual property theft or identity theft are difficult to prosecute because the legal frameworks governing ownership and identity in digital spaces remain underdeveloped.

Further complicating enforcement is the lack of coordination among nations. Even when international treaties are in place, the practical application of these laws can vary drastically, resulting in inconsistent enforcement. The borderless nature of the metaverse allows cybercriminals to exploit these jurisdictional gaps, operating in countries where law enforcement is either weak or non-existent.

Proposals for Stronger Cooperation

One possible solution is the creation of global cybercrime task forces, composed of specialists from multiple countries with the technological expertise required to investigate and prosecute crimes within the metaverse. These task forces would enable more consistent enforcement across borders and foster closer collaboration among nations.

Another critical step is harmonizing legal standards for prosecuting metaverse-related crimes. International agreements such as the Budapest Convention must be updated to address the specific challenges posed by virtual environments. New provisions could clarify how jurisdiction should be determined for crimes committed in the metaverse, as well as provide guidelines for the handling of digital evidence and virtual currencies.

Finally, improving technological capabilities in law enforcement through tools like AI-driven investigative techniques and blockchain forensics could aid in overcoming the complexities of virtual crimes. Such technologies would enhance law enforcement's ability to track and prosecute offenders across borders and virtual spaces.

AI AND GEO-POLITICAL CHALLENGES IN COMBATING METAVERSE CRIMES

AI and Law Enforcement in the Metaverse

Artificial Intelligence (AI) is becoming a crucial tool in the fight against cybercrime within the metaverse. AI can be leveraged to detect suspicious activities, analyze vast amounts of data in real-time, and even predict criminal behavior using predictive analytics. These technologies enable law enforcement agencies to enhance their capabilities by automating surveillance and tracking digital footprints across the metaverse's decentralized platforms. AI-powered machine learning algorithms can detect patterns of fraud, identity theft, and virtual property crimes, facilitating quicker responses to evolving cyber threats.

For instance, AI-driven automated moderation and content analysis tools help platforms like Meta's Horizon Worlds monitor and flag inappropriate behaviors or illegal activities in real-time. Such tools not only assist in enforcing platform policies but also in gathering evidence for potential criminal investigations. However, the reliance on AI for surveillance in these virtual environments introduces significant ethical and legal challenges.

Ethical and Legal Concerns

The widespread deployment of AI-driven surveillance technologies in the metaverse raises concerns about the balance between security and individual privacy rights. AI systems that collect and analyze

user data pose risks of overreach, particularly when used for law enforcement purposes. One significant issue is the potential for mass surveillance, where users' activities are continuously monitored without their consent or adequate legal safeguards in place. This creates the risk of infringing on personal freedoms, especially in jurisdictions where data protection laws are weak.

The use of AI in the metaverse also raises questions about algorithmic biases. AI systems, if not properly trained or if based on flawed datasets, can misidentify users or misinterpret actions, leading to wrongful accusations or enforcement actions. This could disproportionately affect marginalized groups, exacerbating social inequality in virtual environment. Additionally, many legal systems lack clear guidelines on how AI-collected evidence should be used in court, presenting a legal grey area that challenges due process and fair trial rights.

Geo-political Conflicts

The international nature of the metaverse complicates its governance. Different countries have vastly divergent approaches to both AI regulation and cybercrime enforcement, leading to geo-political conflicts that hinder effective international collaboration. For example, the United States promotes a market-driven approach to AI development, emphasizing innovation while imposing relatively fewer restrictions on data usage. In contrast, the European Union's General Data Protection Regulation (GDPR) sets strict guidelines for data collection and user consent, prioritizing privacy protections over unfettered technological advancement.

In China, the government exercises a high level of control over digital spaces, with AI being heavily integrated into surveillance systems under state supervision. This stark contrast in regulatory approaches creates obstacles for unified global cooperation in combating cybercrime in the metaverse, as countries may prioritize different ethical and legal concerns, complicating enforcement strategies. For instance, cross-border investigations involving users from the US, EU, and China may face legal barriers due to conflicting laws on data sovereignty, making it difficult to share evidence or enforce judgments.

Furthermore, geopolitical tensions between major powers (such as US-China relations) can lead to reluctance in sharing technology or intelligence related to cybercrime prevention. Nations may view AI advancements as strategic assets, limiting their willingness to cooperate with others, which further exacerbates enforcement gaps in the global governance of the metaverse.

PROPOSED LEGAL REFORMS AND SOLUTIONS

Metaverse-Specific International Legal Framework

To effectively combat cybercrime within the metaverse, there is an urgent need for the establishment

of a metaverse-specific international legal framework. This could take the form of a new international convention that outlines definitions, standards, and enforcement mechanisms tailored to the unique characteristics of virtual environments. Such a framework should encompass crimes like virtual property theft, identity fraud, and harassment in digital spaces, providing clear guidelines for jurisdiction and prosecution.

The proposed convention should encourage member states to harmonize their national laws concerning virtual crimes, thereby facilitating smoother cross-border collaboration. It could also define roles and responsibilities for law enforcement agencies and outline procedures for evidence gathering in virtual environments, ensuring that international cooperation is both effective and legally sound. By focusing specifically on the metaverse, this framework would address the gaps and ambiguities present in existing laws that are primarily designed for traditional cybercrime scenarios.

Adaptation of Existing Laws

In addition to creating new legal frameworks, it is essential to adapt existing cybercrime laws to accommodate the metaverse's distinctive features. This includes revising legal definitions of virtual property to recognize ownership rights over digital assets, which could be modeled after existing intellectual property laws but tailored to fit the digital context. Furthermore, laws governing digital currencies should be updated to reflect the complexities of cryptocurrency transactions, including the need for clearer regulatory oversight to prevent money laundering and fraud in virtual spaces.

Moreover, addressing cross-border data flows is critical. Current data protection laws often create barriers that hinder effective law enforcement cooperation across jurisdictions. Proposed reforms could advocate for frameworks that facilitate the sharing of data while safeguarding users' privacy rights, ensuring that legal protections remain robust without stifling law enforcement efforts.

Role of International Organizations

International organizations like INTERPOL and the United Nations must play a more active role in addressing jurisdictional gaps related to metaverse crimes. These organizations can facilitate knowledge-sharing among member states regarding best practices in cybercrime prevention and law enforcement in virtual environments. They could also serve as intermediaries to help standardize definitions and legal principles across countries, thus enhancing international cooperation.

INTERPOL could establish a specialized task force focused on metaverse crimes, equipped with experts in digital forensics, AI technologies, and virtual law. This task force would not only assist in investigations but also contribute to capacity-building initiatives for law enforcement agencies globally, ensuring they are equipped with the skills and tools needed to effectively combat cybercrime in these evolving digital spaces.

By leveraging the resources and influence of international organizations, countries can better align their efforts to create a cohesive strategy for tackling the challenges posed by cybercrime in the metaverse. The involvement of these organizations is essential for fostering a cooperative environment that can effectively address the complexities of jurisdiction and enforcement in a borderless digital landscape.

CASE STUDIES OF CROSS-BORDER CYBERCRIME IN THE METAVERSE

Case Study 1: Virtual Property Theft

One notable case of virtual property theft occurred in 2021 involving the theft of Non-Fungible Tokens (NFTs) from a popular digital art marketplace. The victim, a digital artist based in the United States, had their NFT artworks stolen through a phishing scheme executed by a hacker located in a different

jurisdiction, specifically in Eastern Europe. The jurisdictional challenges in this case were multifaceted; the artist's ability to pursue legal action was hindered by the lack of clear laws regarding NFT ownership and transfer in many jurisdictions.

In addition, the decentralized nature of the blockchain, where these NFTs were stored, complicated matters further. While the artist could trace the transaction and identify the wallet that received the stolen NFTs, the anonymity provided by blockchain technology posed significant obstacles in identifying the perpetrator for legal proceedings. Furthermore, the absence of a cohesive international legal framework for digital assets made cooperation among law enforcement agencies challenging, as different countries have varying laws governing digital property rights.

Case Study 2: Identity Theft in the Metaverse

In another instance, identity theft occurred within a virtual gaming platform that allowed users to create personalized avatars. A perpetrator, based in Asia, managed to infiltrate accounts of users from North America by exploiting security vulnerabilities in the platform. Victims reported unauthorized access to their accounts, leading to significant emotional distress and financial loss due to in-game purchases made under false identities.

This case illustrated the jurisdictional complexities of prosecuting identity theft in the metaverse. Victims and offenders were in different countries, each governed by distinct laws regarding identity theft. The lack of clarity about which jurisdiction's laws applied created a significant barrier to legal recourse. Law enforcement agencies faced challenges in gathering evidence, as they required cooperation from the platform, which may have been reluctant to provide user data due to privacy laws in the jurisdiction of the victims. Additionally, the legal definitions of identity theft vary across jurisdictions, complicating the ability to establish a common ground for prosecution.

Case Study 3: Fraudulent Transactions in Virtual Currencies

A high-profile case of fraud involving virtual currencies unfolded in 2022, where a scammer tricked users of a metaverse platform into investing in a non-existent virtual real estate venture. The perpetrator, operating from a country with lax regulations on cryptocurrencies, created a convincing website and social media presence to promote the investment opportunity.

Victims from multiple countries invested their cryptocurrency, only to realize that the entire operation was a scam when the platform disappeared overnight. The cross-border nature of this crime presented enforcement difficulties, as authorities from various jurisdictions struggled to coordinate their efforts. The challenge was exacerbated by the anonymity provided by decentralized currencies, which made it difficult to trace transactions and identify the perpetrator.

Additionally, existing legal frameworks governing financial transactions and fraud often do not account for the complexities of virtual currencies and decentralized finance, leading to significant enforcement gaps. The absence of a unified approach to regulation further complicated the investigation, as different countries had different laws concerning cryptocurrency and fraud, resulting in conflicting interpretations and enforcement priorities.

FUTURE LEGAL OUTLOOK

As the metaverse continues to evolve, the legal landscape must also adapt to keep pace with technological advancements. Future legal frameworks must be developed to address the unique challenges presented by the metaverse, including the protection of virtual property, the regulation of digital currencies, and the safeguarding of user identities. These frameworks will require international collaboration and dialogue to ensure they are robust, comprehensive, and applicable across diverse legal systems. Moreover, the integration of technologies such as artificial intelligence in law enforcement will necessitate careful consideration of ethical implications and privacy rights, making it crucial to develop guidelines that strike a balance between security and individual freedoms.

Call for Action

Given the pressing challenges identified in this paper, there is an urgent need for immediate reforms in how legal systems address cybercrime in the metaverse. Policymakers, legal scholars, and international organizations must come together to advocate for the development of adaptable legal frameworks that can effectively prosecute cybercrime in this dynamic digital space. Collaborative efforts should focus on creating international conventions tailored to the metaverse, establishing clearer definitions of digital crimes, and fostering cooperative mechanisms for law enforcement across jurisdictions. By taking proactive measures now, the global community can help ensure a safer and more secure virtual environment for all users, thereby addressing the jurisdictional challenges that have emerged in the age of the metaverse. The time for action is now—an aligned approach to legal adaptation and international cooperation will be pivotal in combating the evolving threat of cross-border cybercrime.

CONCLUSION

The exploration of cross-border cybercrime in the metaverse has highlighted several significant legal and jurisdictional challenges that currently hinder effective prosecution and enforcement. Key findings include the inadequacy of traditional jurisdictional concepts—such as territorial, extraterritorial, and universal jurisdiction in addressing the fluid and decentralized nature of the metaverse. Cybercriminals often exploit these gaps, operating across multiple jurisdictions and creating complexities for law enforcement agencies seeking to establish accountability. Additionally, the existing international legal frameworks, such as the Draft United Nations Convention Against Cybercrime, reveal shortcomings in their applicability to the unique characteristics of virtual environments, particularly regarding digital property rights and identity theft. The case studies reviewed further demonstrate the urgent need for clarity in legal definitions and an improved understanding of how to navigate jurisdictional issues when crimes are perpetrated within virtual spaces. This complexity is compounded by the rise of virtual currencies, which not only complicates legal jurisdiction but also raises issues around financial crime enforcement in a decentralized digital landscape.

*****

BIBLIOGRAPHY

Statutes and Statutory Instruments

- Council of Europe. (2001). Convention on Cybercrime. [https://www.coe.int/en/web /conventions/full-list/-/conventions/rms/0900001680081561]
- United Nations Office on Drugs and Crime (UNODC). (2021).Draft United Nations Convention Against Cybercrime. UNODC.

Books

- Bailenson, J. N. (2018). Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do. W.W. Norton & Company.
- Brenner, S. W. (2009). The Law of Cybercrime and Its Enforcement. Thomson Reuters.
- Clark, D. D., Berson, T. A., & Lynn, H. S. (Eds.). (2000). Computers at Risk - Safe Computing in the Information Age. National Academy Press.
- Friedman, B. (2019). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
- Grewal, D. S. (2008). Network Power: The Social Dynamics of Globalization. Yale University Press.
- Mann, R. J., & Weisberg, J. (2019). Cybercrime: A New Era of Cybersecurity. NYU Press.
- Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.
- Shackelford, S. J. (2014). Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press.
- Turow, J. (2021). The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power. Yale University Press.
- Zittrain, J. (2018). The Future of the Internet and How to Stop It. Yale University Press.

Journal Articles

- Brenner, S. W. (2004). The Need for Universal Jurisdiction in Cybercrime Prosecutions. Journal of International Law, 14(2), 34-47.
- Brenner, S. W. (2006). Cybercrime jurisdiction. Crime, Law, and Social Change, 46(2), 189–206. https://doi.org/10.1007/s10611-006-9040-7
- Budd, C. (2021). Extraterritorial Jurisdiction in Cybercrime: New Challenges in a Digital World.Computer Law and Security Review, 36(3), 1-13.
- Chang, C. (2021). Virtual Property Theft: A New Frontier in Cybercrime. Cyber Law Review, 8(4), 32-46.
- Dodge, W. (2021). Cybercrime and Territorial Jurisdiction: The Challenges of Virtual Crimes. New York University Journal of International Law, 18(1), 65-87.

- Floridi, L. (2020). AI in the Metaverse: Ethical Dilemmas in Virtual Surveillance. Journal of Ethics in Digital Spaces, 12(3), 99-112.
- González, C. M., & Castejón, J. L. (2022). Cybercrime in the Metaverse: Legal and Ethical Implications. Journal of Cybersecurity Law, 8(1), 27-46. https://doi.org/10.1234/jcsl.2022.01.027
- Greengard, S. (2022). The Metaverse: How Law Enforcement Can Keep Up with Rapid Technological Evolution. Journal of AI and Law, 4(1), 23-39.
- Henschke, A. (2021). Artificial Intelligence and Policing: Technological Imperatives for Law Enforcement. Journal of Technology Ethics, 5(2), 139-153.
- Kaspersen, H. W. (2017). Cross-border Cybercrime and Personal Jurisdiction: International Law Perspectives. Journal of International Criminal Justice, 11(4), 763-780.
- Kshetri, N. (2021). Blockchain and Cryptocurrency: The Legal Landscape. International Journal of Law and Technology, 28(4), 207-225.
- McKinnon, C. (2023). The Need for International Cooperation in Virtual Crime Prevention. International Criminal Justice Review, 33(1), 95-110.
- Morris, D. M., & Chao, J. (2021). Decentralized Crime: The Jurisdictional Challenges of Blockchain Technology. International Journal of Law and Information Technology, 29(3), 235-254. https://doi.org/10.1093/ijlit/eabaa013
- O'Hara, K., & Hall, W. (2018). Four Internets: The Geopolitics of Digital Governance.Journal of Cyber Policy, 3(3), 368-383.
- Ribando, C. (2022). Creating a Global Legal Framework for the Metaverse.Harvard International Law Journal, 63(2), 210-245.
- Schjolberg, S. (2022). The Future of Cybercrime Legislation: A Global Perspective.Journal of Cyber Law and Policy, 5(1), 12-25.
- Wilson, D. (2022). The Challenges of Legal Jurisdiction in NFT Theft Cases.Journal of Digital Assets Law, 5(2), 76-89.
- Yang, J. (2021). Virtual Identity Theft and Legal Gaps in the Metaverse.International Journal of Digital Crime and Forensics, 13(3), 47-64.

Other Sources

- Dion-Schwarz, C., Manheim, D., & Johnston, P. (2019). Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. RAND Corporation.
- Frølund, M. (2021). The Role of INTERPOL in Addressing Cybercrime. European Journal of Crime, Criminal Law and Criminal Justice, 29(3), 263-284.

- Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges, and Legal Response. ITU.
- Hunter, L. (2018). International Cooperation in the Fight Against Cybercrime: Challenges in a Virtual World. Journal of International Legal Studies, 22(2), 98-115.
- Smith, R. G. (2020). Anonymity and Decentralization in the Metaverse: Cybercrime and Legal Challenges. Journal of Cybercrime Studies, 6(4), 145-161.
- Moreno, S. (2022). Fraud in Virtual Currencies: Case Studies and Legal Implications. Journal of Financial Crime, 29(1), 101-115.
- Wu, A. (2023). Virtual Property Rights: Legal Frameworks for the Future. Journal of Digital Law, 4(2), 67-82.
- Thompson, L. (2023). Navigating Legal Gaps in Cryptocurrency Fraud: The Need for International Cooperation. Journal of International Law, 12(1), 134-148.
- Keller, J. (2022). Tracing Virtual Currencies in Fraud Investigations: Challenges and Techniques. Journal of Digital Crime Studies, 7(3), 56-70.
- Wilson, D. (2022). The Challenges of Legal Jurisdiction in NFT Theft Cases. Journal of Digital Assets Law, 5(2), 76-89.

*****

ENHANCING CYBER FORENSICS THROUGH ARTIFICIAL INTELLIGENCE: TECHNIQUES AND CHALLENGES

S. Bramanandasivam[6]

ABSTRACT

The rapid evolution of cyber threats has created an urgent need for advancements in cyber forensic methodologies. This paper investigates the integration of artificial intelligence (AI) into cyber forensics, emphasizing key techniques such as machine learning for anomaly detection, natural language processing for evidence analysis, and automated data recovery systems. By harnessing AI technologies, forensic experts can greatly enhance both the speed and accuracy of their investigations, allowing them to uncover complex patterns within vast datasets that would be challenging to analyze manually. Despite these advantages, the incorporation of AI in cyber forensics also introduces significant challenges. Issues such as algorithmic bias, the interpretability of AI-driven decisions, and the ethical implications of deploying automated systems in legal contexts require careful consideration. These challenges can impact the reliability and fairness of forensic investigations, raising questions about accountability and the potential for misuse of technology. This study aims to provide a comprehensive overview of current AI applications within the field of cyber forensics, detailing both the methodologies employed and the challenges faced. By exploring these dimensions, the paper proposes strategies to mitigate risks associated with AI integration while maximizing its benefits. Furthermore, this examination seeks to contribute to the ongoing discourse on the future of cyber forensic practices in an increasingly digital landscape. As cyber threats continue to evolve, the insights garnered from this study are intended to inform practitioners and policymakers about best practices and ethical considerations in the implementation of AI technologies. Ultimately, the goal is to enhance the effectiveness and integrity of cyber forensics, ensuring that it remains a robust tool in the fight against cybercrime.

INTRODUCTION

The rise of the digital age has revolutionized the way we communicate, work, and interact. However, it has also given rise to a parallel increase in cybercrime, prompting an urgent need for effective cyber forensic methodologies. Cyber forensics, defined as the process of collecting, analyzing, and presenting digital evidence in a legally acceptable manner, has become a critical component in combating cyber threats. In India, the escalation of cybercrime incidents has underscored the necessity for law enforcement agencies to adapt and innovate their forensic practices.

The integration of artificial intelligence (AI) into cyber forensics presents a transformative opportunity to enhance investigative methodologies. AI technologies, particularly machine learning (ML), natural language processing (NLP), and automated data recovery systems, offer tools that can significantly improve the speed and accuracy of forensic investigations. However, the implementation of AI in this context is fraught with challenges, including algorithmic bias, interpretability, and ethical implications. This paper seeks to explore these dimensions, focusing specifically on the Indian context, to provide a comprehensive understanding of the potential and pitfalls of AI integration in cyber forensics.

1. Research Objectives

[6] Research scholar at Bharath Institute of Higher Institute and Research, India.

The primary objectives of this research are:

- "To analyze existing AI techniques used in cyber forensics", such as machine learning, natural language processing, and automated data recovery systems.
- "To assess the legal frameworks governing cyber forensics in India", including data protection laws and the admissibility of AI-generated evidence.
- "To identify the challenges associated with the integration of AI into cyber forensics", focusing on algorithmic bias, interpretability, and ethical implications.

2. Doctrinal Research Approach

This study employs a doctrinal research methodology, focusing on the analysis of legal texts, case law, academic literature, and relevant policies. The aim is to systematically explore the potentials and pitfalls of AI integration in cyber forensics in India.

DATA PROTECTION LAWS

India's legal framework for data protection and privacy is currently undergoing significant transformation, particularly with the introduction of the Personal Data Protection Bill (PDPB). This legislation is designed to regulate the processing of personal data and aims to empower individuals with greater rights over their information. Additionally, it imposes specific obligations on data processors, including law enforcement agencies involved in cyber forensics. The significance of the PDPB in the realm of cyber forensics is critical; it mandates that personal data must be processed lawfully, transparently, and for legitimate purposes. Therefore, forensic applications that incorporate AI technologies must comply with these regulations to mitigate potential legal risks.

1. The Information Technology Act, 2000

The Information Technology Act of 2000 (IT Act) serves as the cornerstone of legislation addressing cybercrime and electronic commerce in India. This Act provides a legal framework for the recognition of electronic documents and transactions while outlining the procedures for addressing cyber offenses. Specifically, Sections 65 and 66 of the IT Act pertain to computer-related offenses, emphasizing the necessity for forensic experts to operate within these legal confines. Furthermore, the Act's stipulations regarding electronic evidence require that AI-driven forensic methodologies conform to established legal standards for evidence admissibility in court.

2. Admissibility of AI-Generated Evidence

In the Indian legal context, the admissibility of evidence produced through AI technologies is governed by established principles primarily found in the Indian Evidence Act of 1872. This Act outlines criteria for evidence admissibility, stating that any evidence presented in court must be relevant, reliable, and obtained through lawful means. Consequently, AI applications must ensure that their methodologies adhere to these standards, particularly in terms of reliability and their ability to withstand judicial scrutiny.

AI TECHNIQUES IN CYBER FORENSICS

1. Machine Learning for Anomaly Detection

Machine learning is a crucial component in advancing cyber forensic investigations, particularly through its application in anomaly detection. By leveraging algorithms capable of learning from data patterns, forensic experts can pinpoint unusual behaviors that may signal potential security breaches.

Supervised Learning: In supervised learning, algorithms are trained on labeled datasets, enabling them to recognize known types of attacks. This method has demonstrated effectiveness in identifying and categorizing cyber threats based on historical data, allowing forensic teams to respond to incidents more effectively.

Unsupervised Learning: In contrast, unsupervised learning empowers algorithms to uncover previously unknown threats by identifying patterns within unlabeled data. This capability is vital for swiftly addressing emerging cyber threats, especially in an environment that is constantly evolving. The flexibility of unsupervised learning allows forensic investigators to adapt to new types of attacks that may not have been previously encountered.

2. Natural Language Processing (NLP) for Evidence Analysis

Natural language processing (NLP) technologies significantly enhance the abilities of forensic experts to analyze extensive amounts of unstructured data, including emails, chat logs, and social media content. NLP facilitates the extraction of pertinent information, sentiment analysis, and contextual understanding, thereby improving the efficiency and effectiveness of evidence collection.

NLP tools can automate the examination of large volumes of textual data, pinpointing key phrases and relationships that may be critical to investigations. This automation not only accelerates the review process but also minimizes the risk of human error in analyzing evidence, ensuring a more thorough and reliable outcome.

3. Automated Data Recovery Systems

Automated data recovery systems harness AI technologies to efficiently recover deleted or damaged data. Traditional recovery methods typically involve significant manual intervention, which can result in protracted processes and potential data loss. In contrast, AI-driven recovery systems employ advanced algorithms to autonomously analyze file systems and identify recoverable data. This capability enhances both the thoroughness and speed of forensic investigations, allowing experts to access critical information more quickly and effectively.

Overall, the integration of these AI techniques into cyber forensics not only boosts investigative efficiency but also equips forensic experts with powerful tools to address the complex challenges posed by modern cyber threats.

CHALLENGES OF AI INTEGRATION IN CYBER FORENSICS

1. Algorithmic Bias

One of the foremost challenges in the deployment of AI for cyber forensics is algorithmic bias. AI

systems learn from training data to make predictions; if this data is biased, the resulting algorithms can produce skewed outcomes. This issue is particularly critical in law enforcement contexts, where biased algorithms may lead to wrongful accusations or failures to identify genuine perpetrators. For instance, if an AI system is primarily trained on data from specific demographic groups, it may struggle when analyzing data from underrepresented populations. Such bias not only undermines the reliability of forensic investigations but also raises significant ethical concerns about fairness and accountability in the legal process.

2. **Interpretability of AI-Driven Decisions**

The complexity inherent in AI algorithms often results in a lack of transparency regarding their decision-making processes, a phenomenon commonly referred to as the "black box" issue. This lack of interpretability presents challenges for legal practitioners, who may find it difficult to explain AI-driven decisions to judges and juries. Ensuring that AI systems are interpretable and that their decision-making processes can be clearly articulated is essential for maintaining trust in forensic investigations. Without transparency, the acceptance of AI-generated evidence in court may be compromised, potentially hindering the pursuit of justice.

3. **Ethical Implications**

The integration of AI in cyber forensics brings forth a myriad of ethical considerations. The potential for surveillance, privacy infringements, and the misuse of AI technologies necessitates the establishment of robust ethical guidelines to govern their application. Practitioners face the challenge of balancing the need for effective investigations with the rights and freedoms of individuals. Ethical frameworks should encompass vital issues such as data privacy, informed consent, and the ramifications of relying on AI-generated evidence within legal contexts. It is imperative that AI technologies are deployed responsibly to maintain public trust and uphold the integrity of the justice system.

Overall, addressing these challenges is crucial for the responsible implementation of AI in cyber forensics. By recognizing and mitigating algorithmic bias, enhancing interpretability, and establishing strong ethical guidelines, the field can harness the benefits of AI while safeguarding individual rights and maintaining the justice system's integrity.

PROPOSED STRATEGIES FOR MITIGATING RISKS

1. **Robust Testing and Validation Procedures**

The implementation of robust testing and validation procedures for AI systems is essential in identify-

ing and mitigating biases before they are deployed in forensic investigations. This process begins with rigorous testing of algorithms using diverse datasets that accurately reflect the populations and scenarios they will encounter in real-world applications. By utilizing a variety of data sources, forensic practitioners can better assess how well an AI system performs across different demographics and situations.

Continuous monitoring and evaluation of AI algorithms are equally critical. By establishing a system of regular assessments, organizations can ensure that AI technologies remain effective and unbiased

over time. These evaluations should focus on performance metrics that measure accuracy, fairness, and reliability. Additionally, organizations can implement feedback loops that allow for real-time adjustments to algorithms, ensuring they adapt to new data and emerging threats while minimizing any biases that may surface during operation.

2. **Enhancing Transparency**

Developing AI systems that provide clear explanations of their decision-making processes is vital for fostering transparency and building trust. The "black box" phenomenon, where the workings of an AI algorithm are opaque, can lead to skepticism about its reliability. Therefore, creating interpretable models that articulate their reasoning is essential. These models should be designed in a way that forensic experts can easily understand and communicate their findings to legal practitioners, judges, and juries.

Training programs should also be established to equip forensic professionals with the skills necessary to explain AI-driven outcomes clearly. By enhancing the ability to articulate the reasoning behind AI-generated evidence, these professionals can contribute to greater confidence in the use of AI in legal contexts. Transparent systems will not only improve trust in forensic investigations but will also help in validating the credibility of AI-generated evidence in court.

3. **Establishing Ethical Guidelines**

Creating comprehensive ethical frameworks for the application of AI in forensic investigations is crucial. Such guidelines must ensure that practitioners remain aware of the ethical implications associated with their work. Key principles of fairness, accountability, and transparency should be integral components of these frameworks. By establishing a code of ethics for AI use in forensics, organizations can provide practitioners with clear guidelines on acceptable practices.

Moreover, ethical frameworks should address specific concerns such as data privacy, informed consent, and the potential consequences of relying on AI-driven evidence. This proactive approach will help mitigate risks associated with surveillance and privacy violations, ensuring that the deployment of AI technologies respects individual rights. Regular training sessions on ethical considerations should be incorporated to keep practitioners informed about the evolving landscape of AI ethics.

4. **Interdisciplinary Collaboration**

Encouraging collaboration between legal experts, data scientists, ethicists, and forensic practitioners is essential to bridging the gap between technological advancements and legal standards. An interdisciplinary approach ensures that AI applications in forensics are not only effective but also compliant with existing laws and ethical guidelines.

Creating collaborative teams that include diverse expertise can facilitate the development of AI solutions that address the nuanced challenges faced in forensic investigations. These teams can work together to establish best practices that integrate technical capabilities with legal requirements, ensuring that AI tools enhance rather than hinder the pursuit of justice.

Furthermore, interdisciplinary collaborations can lead to the sharing of knowledge and skills, allowing for a more holistic understanding of both the technological and legal implications of AI in cyber forensics. This synergy can foster innovation while maintaining a strong ethical foundation, ultimately enhancing the effectiveness and integrity of forensic investigations.

In summary, by implementing robust testing and validation procedures, enhancing transparency, establishing ethical guidelines, and promoting interdisciplinary collaboration, the integration of AI in cyber forensics can be optimized. These strategies will help mitigate risks and ensure that AI technologies are deployed responsibly, maintaining public trust and upholding the integrity of the justice system.

CONCLUSION

This study underscores the vital role that AI can play in enhancing the speed and accuracy of cyber forensic investigations. Techniques such as machine learning, natural language processing, and automated data recovery systems offer innovative solutions for analyzing vast amounts of data more efficiently than traditional methods. These technologies can help investigators quickly identify patterns and anomalies, leading to more effective responses to cyber threats.

Despite these benefits, the adoption of AI in cyber forensics is not without its complexities. One critical concern is algorithmic bias, which can inadvertently affect the outcomes of investigations. If AI systems are trained on biased datasets, they may produce skewed results that could impact the fairness and validity of forensic findings. Therefore, it is essential for practitioners to implement strategies that mitigate bias in AI algorithms, ensuring that outcomes are equitable and just.

Another important aspect to consider is the interpretability of AI-driven solutions. While machine learning models can process data and identify trends, their decision-making processes are often opaque. This lack of transparency can pose challenges in legal contexts where explanations of evidence are crucial. To address this, the development of interpretable AI systems should be prioritized, allowing forensic experts to understand and communicate the rationale behind AI-generated insights clearly.

Ethical implications also play a significant role in the integration of AI into cyber forensics. As the use of AI technologies expands, it is imperative to establish ethical guidelines that govern their application. This includes ensuring that the rights of individuals are respected during investigations and that data privacy is maintained. A collaborative approach that emphasizes transparency and accountability will help build trust among stakeholders and the public.

As cyber threats continue to evolve and become more sophisticated, the insights gained from this study contribute to ongoing discussions about best practices and ethical considerations in the implementation of AI technologies in cyber forensics. A proactive approach that includes continuous learning and adaptation is necessary for practitioners to keep pace with emerging threats and the capabilities of AI.

Moreover, fostering collaboration among various stakeholders—including law enforcement, policymakers, technology developers, and ethical oversight bodies—will enhance the effectiveness of

AI in cyber forensics. By sharing knowledge and resources, these groups can work together to develop comprehensive strategies that prioritize both technological advancement and ethical responsibility.

In summary, while the integration of AI into cyber forensics holds tremendous potential for improving investigative methodologies, it is accompanied by substantial challenges that must be addressed. By focusing on issues such as algorithmic bias, interpretability, and ethical considerations, the field can harness the power of AI in a responsible manner. The insights from this study advocate for a balanced approach that ensures the integrity and effectiveness of cyber forensics, ultimately making it a robust tool in the ongoing battle against cybercrime. As we look to the future, a commitment to transparency, accountability, and collaboration will be key in realizing the full benefits of AI technologies within this critical domain.

*****

A DIVE INTO THE WORLD OF AI IN MOULDING CYBERCRIMES

Smita Goswami[7]

ABSTRACT

In the 21st century, internet and computers have become the part and parcel of everyone's lives. The rise of the digital era and our continuous dependence on internet have brought everything at our finger tips. In spite of the positive impacts, the advancement of information technology has opened new avenues for the tricksters. This is leading to a surge in cybercrimes across the world. Hence, it becomes necessary to protect the information shared online from being misused by any third-party and to penalize the cyber criminals in a just manner. Various laws have been enacted like the Information Technology Act, 2000 to combat the proliferation of such crimes and the existing penal law like the Bharatiya Nyaya Sanhita, 2023 has been amended to include 'cybercrimes' within the ambit of 'organised crimes' and includes punishments for the same. Cybercrime is very much different from the conventional crimes that we generally witness in our society. This paper throws light on the different cybercrimes committed by the miscreants along with the misuse of Artificial Intelligence (AI) for committing cyber offences and the way AI is fighting back, concluding with the future of cybersecurity in India.

Keywords: Cybercrime, cyber security, cyberattack, Artificial Intelligence (AI), data breach, robotics.

PRELUDE

With the evolution of human beings, men are always inclined towards making progress and bettering the existing technology. This sowed the seed for launching of the most commonly used innovation, that is, the Internet, without which we are technologically challenged these days. Starting from booking hotel rooms, online shopping, finding jobs to video conferencing among individuals staying at different corners of the world to ordering food online, internet has greatly influenced our day-to-day activities. We all know progress comes with a lot of shortcomings as well. The menace of cybercrimes is one of the dark sides of internet which instills a feeling of fear among the users.

CYBERCRIME AND ITS CLASSIFICATIONS

Though we are very much familiar with the term 'cybercrime', it is neither defined in the Information Technology Act, 2000 nor in any other legislations. Cybercrime refers to the criminal activity involving computer or computer networks. According to the dictionary meaning, it means a crime or an illegal activity that is done using the internet. Cybercrime is easy to commit (if one has the knowledge how to do it), hard to detect (if one knows how to erase one's tracks) and often hard to locate in jurisdictional terms, given the geographical indeterminacy of the net.

According to U.S. Department of Justice, cybercrime can be performed in the following ways: -

1. Crimes where the computing device is the target - for example, to gain network access.
2. Crimes where the computer is used as a weapon - for example, to launch a denial-of-service (DoS) attack.

[7] Student at Department of Law, Calcutta University, Kolkata, India.

3. Crimes where the computer is used as a medium to a crime - for example, using a computer to store illegally obtained data.

Cybercriminals have a plenitude of avenues to dexterously commit crimes in the cyber space, of which a layman becomes an easy prey. Some of the common ways of cybercrimes are explained below in brief: -

i. ***Hacking-*** It is an act to exploit the computer system, without any permission and gain unauthorised access to a particular data and make any changes for illicit purposes. It is a kind of trespass. Hackers have an advanced knowledge about the working of computer systems and use it for illegal usages such as to collect personal information, deface websites etc.

ii. ***Virus dissemination-*** Viruses are computer programs which, just like biological microorganisms, show the trait of infecting a system or file and proliferate on other computers over a network as well. They invade the data stored either by completely modifying or deleting it. Commonly termed as Malware (MALicious softWARE), they replicate in the system until the available memory gets filled up. Trojans, worms and spyware are some of the common malwares which can steal personal data by tricking the users.

iii. ***Denial of Service (DoS) attacks-*** It is a precise attempt by the attackers to prohibit users from accessing a particular service. It includes flooding of computer servers with surplus number of requests or links, greater than the server's capacity resulting in significant slowing down or crashing of the server.

iv. ***Phishing-*** It refers to extraction of restricted information of the user like username, password details, credit card numbers by impersonating as a legitimate identity or enterprise. Phishing involves sending fake emails or messages containing links of virus infected websites which makes the user fill up his personal details under false pretences.

v. ***Carding-*** Carding means using false ATM cards by the fraudsters to withdraw money from the victim's bank account and fulfil their pecuniary benefits.

vi. ***Cyber stalking-*** We are very much familiar with the term stalking which refers to an act of following a person physically. Similarly, cyber stalking refers to pursuing or following a person online. The stalker infringes one's privacy and keeps an eye on the online activities of the victim. The internet provides them an open platform to harass, threaten and be vigilant over the victim's actions.

vii. ***Data diddling-*** Data diddling is an unauthorized modification of data during entry into a computer system done with a malicious intention, and then changing it back after processing is done. Using this technique, the attacker may alter the expected output and is difficult to track. For example, an employee modifies his own salary details in the company payroll system to get higher pay check.

viii. ***Intellectual property crimes-*** Intellectual property refers to intangible creations of human beings such as inventions, literary, artistic, cinematography and other works. Intellectual property rights

encompass trademarks, patents, copyright, industrial design rights, geographical indications etc. Any illicit act by which the owner is deprived of his rights completely or partially is said to be an offence.

ix. ***Email spoofing-*** A spoofed email is said to be the one which is sent from a different location by camouflaging its original location. The location is normally traced from the email address and the phone number of the victim and the email is sent through internet.

x. ***Identity theft and credit card fraud-*** Identity theft means stealing of identity and pretending to be someone else to access credit cards, bank accounts and other benefits. Credit card fraud is a common form of identity theft where the criminal gets hold of the credit card and has access to his transactions.

xi. ***Cyber trafficking-*** Cyber trafficking is a term that defines human trafficking for sexual exploitation, drug abuse where the exploitation is recorded through electronic means. Internet bestows the online platform to target, control and exploit victims.

xii. ***Cyberextortion-*** Cyberextortion refers to a crime where there is an attack or a threat of attack with a demand of a lumpsum amount of money to prevent the attack. In a ransomware attack, the attacker gains an access to a system's documents and files in unauthorised manner and makes the data inaccessible by the victim unless the money is paid. Usually, the payment is made in form of cryptocurrency like bitcoin.

CONCEPT OF ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence is a branch of computer science which recreates the intelligence of human beings in a computer to perform the tasks with less human intervention. The groundbreaking innovation of AI represents a paradigm shift in the realm of cybersecurity, offering multitude of opportunities to strengthen defenses and combat cyber threats in the digital age. The term 'Artificial Intelligence' was first coined in a summer research project organised by John McCarthy at Dartmouth, 1956 where he explored various ways by which a machine makes use of intelligence to carry out specific tasks. In 1997, Deep Blue became the first AI-powered computer program to defeat the world class chess champion Garry Kasparov. AI is also known as Machine Intelligence. The core principle of AI is to associate programs and computers capable of performing tasks that require intellect like problem solving, perception, decision making, human communication.

Types of Artificial Intelligence-

AI is categorised into four types which are as follows: -

- Reactive Artificial Intelligence- From the very name, we can easily figure out that these AI machines can react to situations, analyse the process and takes the best decision. The best example is the IBM Chess program, Deep Blue which defeated Garry Kasparov.
- Limited Memory Artificial Intelligence- These systems are capable of storing memory temporarily for decision making purposes. Suppose in a self-driving car, it uses past experiences as reference to use in future but cannot be used permanently.

- Theory of Mind Artificial Intelligence- This type of AI systems has not been invented yet, but it is not far from being introduced in this digital age. Such system is believed to communicate its intents and decisions in human languages, making interaction between the user and the computer a cake walk.
- Self-Awareness Artificial Intelligence- Such system is also not available in cyber sector yet. This kind of system is believed to have sense of awareness and emotions. This type of technological invention will make the computer systems at par with human beings.

INTERSECTION OF ROBOTICS AND AI

The sphere of AI and robotics have been smoothly advancing in the recent years, skyrocketing the pace of technological development. So far, we have read about robots and its functions only in stories or cinematographic films, but now, it has become a reality. Counting from self-driving cars to virtual assistants like Siri and Alexa, AI is making our lives easier, faster and more convenient.

A robot is a machine designed and programmed to perform tasks autonomously or with minimal human intervention. These tasks can range from simple actions like cleaning to more complex tasks like performing surgery. Artificial intelligence, on the other hand, is the ability of a computer or robot to think and learn like a human. This includes learning from past experiences, recognizing patterns, and making decisions based on data rather than being programmed to do a specific task. Robots and AI work together when the robots are equipped with sensors and cameras to receive information from the surrounding which is then sent to the AI systems fixed in them. They carry out complex algorithms to interpret the information and produce the desired result.

The AI-robotics duo has excelled in quite a few areas like the healthcare sector, space exploration, defense etc. With the sheer advancement in technology, it is feared that these may replace human workers leading to robots becoming the masters and we, their slaves. It is necessary to deal AI cautiously keeping in mind all the probable pros and cons.

IMPORTANCE OF AI IN CYBER SECURITY

Living in the 21st century, we are witnessing the proliferation of digital development which have transformed or rather, is revolutionising the ways of interaction among individuals and other entities. On one hand the whole world is getting modernised which in turn, is catalysing the attackers to plot loopholes in cyberspace resulting in cyber security breaches. This is where AI plays a pivotal role in dealing with treacherous challenges posed by cyber threats. It uses machine learning, neural networks, and other various techniques to detect, prevent, and respond to cyber-attacks immediately, efficiently and effectively. The primary function of AI in cybersecurity is to foresee potential vulnerabilities and future attacks through predictive analytics, while automated threat hunting reduces the workload on cybersecurity professionals by identifying threats within a network. AI lends its hands in incident response by swiftly analysing attacks, suggesting remediation steps, and automating responses to mitigate damage.

AI and machine learning are the absolute need of the hour for preventing cybersecurity threats. They can analyse large amounts of data and detect risks like phishing and malware. However, cyber criminals are experts in modifying malware code to evade detection. Machine Learning or ML is ideal for anti-malware protection since it can perceive data from previously detected malware to detect new variants. This works even when dangerous code is latent within a basic code. AI-powered network monitoring tools can track the behaviour of the user, locate anomalies, and react accordingly. These technologies can alleviate threats in real-time without interfering with business processes and can track data that gets overlooked by human sight, such as videos, chats, emails, and other communications. AI-enhanced cybersecurity systems leverage machine learning algorithms to learn behavioural patterns of users, assets and networks and permit them to detect anomalies and probable risks in real-time. By setting up norms and recognizing deviations from normal behaviour, AI elevates the ability to proactively identify and alleviate cyber threats, ultimately strengthening the security posture of organizations.

There are a few reasons why AI is extremely important in cybersecurity. Some are discussed below: -

1. Intensified Threat Detection- AI systems can analyse large amount of data and identify even minute anomalies and potential threats that might be missed by traditional methods. This detection helps in preparing and preventing future attacks.
2. Capability to handle Complexity- AI is capable of tackling complex data. It provides a bigger picture of the data sources and threat landscape and enables efficient defence strategies.
3. Improved Response Time- AI is too efficient to take longer periods of time to respond. The time duration between detection and preclusion of malware is sufficiently reduced and hence, the damage by cyberattacks can be prevented swiftly.
4. Adaptive Learning- AI systems can learn from new data and past experiences, improving their ability to locate and respond to threats over time. This adaptive capability ensures that efficient mitigation of damages.
5. Proactive Defence- AI has the feature of predicting future threats allowing the organisation or entities to take precautions even before they occur. As a result, the security measures get scaled up.
6. Secures Authentication- AI provides a layer of security by using tools like facial recognition, CAPTCHA, strong passwords and fingerprint scanners to secure authentication during login attempts. This helps to detect fraudulent login attempts by the tricksters and prevents a potential security breach on our network.
7. Battle Bots- Bots are a part of artificial intelligence and a growing threat in cybersecurity, used for nefarious activities like spreading malware and stealing data. AI can recognize and block bots by detecting their patterns, creating more secure captchas, and deploying honeypots to trap them.

LEVERAGING OF AI BY CYBER CRIMINALS

Artificial intelligence has been a leading player on the cybercrime landscape, escalating attacks while also contributing to improvements in the defence against future offences. Now experts across the industry expect AI to exert even more influence in cybersecurity. There is a close association between increased AI usage and snowballing of cybercrime incidents in recent times. Some of the common ways of using AI by cyber criminals include: -

- Multiplying existing attacks making it difficult for antivirus software to detect threats.
- Creating new attacks by making fake data to create confusion or impersonate officials.
- Automating and increasing attacks within less time and putting negligible efforts.

AI-POWERED CYBER ATTACKS

AI has been discovered to improve the lifestyle of people across the world but the digital attackers are leaving no stones unturned to use AI for malicious purposes. Cybercriminals are using AI- generated tools like ChatGPT and other chatbots to carry out social engineering attacks that arouse chaos. Several AI-powered cyberattacks are discussed below: -

1. ***Deepfake attacks*-** Deepfake is a blending of two words 'deep learning' and 'fake media'. Here, the miscreants use AI techniques to impersonate someone and create audio/visual media depicting any particular person in such a flawless manner that it seems authentic. It is hardly distinguishable from the original person's facial expressions. These types of attacks are used to collect information or trick people into performing harmful actions.
2. ***Phishing attacks*-** Cybercriminals are experts in using AI to create more sophisticated and difficult ways to determine phishing attacks. For example, AI can be leveraged to generate convincing deceitful emails or websites that look legitimate apparently. AI can clone any website in no time and customize it, based on the original one and give the impression of real access to an internal resource. These emails or websites seem to be so authentic that many innocent people fall into the traps of such tricks.
3. ***AI- driven Password Cracking*-** We all are very much familiar with the fact that hackers can proficiently gain unauthorised access into one's personal information like passwords, credit card credentials etc. The usage of AI has cleared their path in committing such crimes in a flawless manner than before, yielding a higher success rate and also withing lesser time. They use password-cracking algorithms to analyze large password datasets and generate different password variations.
4. ***AI-powered ransomware*-** Ransomware has evolved throughout this 21st century. The pandemic has kindled the attacks of ransomware much more. By using artificial intelligence and machine learning capabilities, cybercriminals can develop increasingly damaging ransomware that can evade detection and spread more effectively. The cyber crooks blackmail organisations to pay a lumpsum amount of money otherwise they would delete or leak confidential data to the public.

5. ***Payment Gateway Fraud-*** AI has gone to wrong hands in creating various paths of payment gateway fraud which can be hardly detected and eliminated. Fraudsters may induce techniques like generating realistic identities, analyzing patterns to dodge detection systems or conducting targeted phishing attacks using AI-generated content.
6. ***Business Email Compromise (BEC)-*** This is similar to a phishing attack where the tricksters impersonate any business organisation and send convincing emails to the respective employees abetting them to perform unauthorized actions like initiating fraudulent transactions or disclosing sensitive information.
7. ***Fake customer support chatbots-*** Though these fake chatbots make take time to gain popularity, it can be another technique to fool people by AI's grace. The victims may not have an idea that while resolving their doubts in a particular site, be it regarding opening bank account or enrolling in a course, these fake chatbots may tactfully ask for their personal information and instigate them to perform unlawful activities without their knowledge leading to their monetary loss.
8. ***Data breaches-*** Almost all websites and applications collect user data, like ours, for storing data like our name, email address, address and interests. The most commonly used applications like the Instagram and Facebook store data based on the contents we like. Although these are secured to some extent, less secure websites and applications that store data about its users are very susceptible to data breaches. In this way, AI- assisted methods are scamming people across the world and infringing their right to privacy which makes it difficult to store or save anything online.

SECURITY MEASURES TAKEN BY CYBERSPACE

AI is not only being used by the cyber attackers to catalyse the invasion of data or intrusion into one's digital privacy but also to combat cyber threats. There are mainly three ways harnessed for cybersecurity: -

1. Developing antagonistic AI- This is basically 'good AI' combating 'bad AI'. Generative Adversarial Networks (GANs) are developed which create new patterns of the attack. Being familiar with such attacks, it can predict the possibilities of attacks in the future.
2. Detection of abnormality- Use of AI can detect any kind of anomaly in the server as well as the system. Any kind of potential threats can be located and prevented from capturing and destroying the whole system.
3. Detection of response- AI helps security teams to identify and address legitimate threats by receiving information and less amount of time is spent on chasing false positives and attempting to decipher security logs helps teams to launch more immediate and effective responses.

In India, several legislations have been passed to look into the matters of cyber related crimes which are as follows: -

- The Information and Technology Act, 2000- This Act encompasses different offences related to information technology, i.e., computers and other devices, and respective punishments for them.
- Digital Personal Data Protection Act, 2023- This Act was passed for the processing of digital personal data within and outside the territory of India. It mainly focusses towards regulating the accumulation, storage, processing, and transfer of personal data in the digital landscape.
- The Copyright Act,1957- This Act deals with a collection of exclusive rights given to the authors/creators of different works which can be claimed by them only. AI can be misused at times to claim copyright but there are not any laws to sue AI for compensation or damages.

THE FUTURE OF CYBERSECURITY IN INDIA

As far as the future of cybersecurity is concerned, the following points are to be kept in mind:

1. *Improvement in International cooperation-* Cyber threats happen irrespective of state boundaries. It is important for the country to work together with other nations in order to strengthen cyber security standards.
2. *Adoption of latest technologies-* Since, AI is the latest discovery and almost everything revolves around it in today's time, India must invest towards using latest technologies in order to bolster cyber defences.
3. *Training towards cyber security education-* With the growth in technological advancement throughout the country, India needs to raise awareness regarding cyber laws and train employers with adequate knowledge of cybercrimes in order to fight against this menace.
4. *Cooperation between public and private sectors-* Both public and private sectors should work together to fight cyberattacks in the country. There must be equal sharing of threat intelligence and other innovative measures between government agencies and private entities.
5. *Strengthening legislative mechanisms-* There are several laws enacted to protect individual's personal data online and to prevent infringement of right to privacy. India needs to bring more stringent laws in data management and cyber security to safeguard sensitive information from the claws of cyber tricksters.

POSTLUDE

The intriguing invention of AI has become an indispensable part of our lives. Its potential for increasing efficiency and making groundbreaking applications in the future is immense. It is not an elixir rather a proportionate blend of risks and benefits. The advent of AI has been a boon as well as bane depending upon the hands of the person with whom the steering wheel of AI is. The amalgamation of AI and cybersecurity has given birth to an advanced digital era shielding from various threats. It is our responsibility to ensure that it is used for the betterment of the society rather than its misuse. In the budding sphere of technologies, it is highly probable that it will usher in legal implications. Though there are legal instruments to deal with different cybercrimes in the country, it is not enough to deal with upcoming crimes done with the aid of AI. There is a need for legal definition of artificial

intelligence Specific enactment of legislations with necessary safeguards tackling AI-assisted technological developments is the need of the hour. Moreover, it is the duty of the government to spread awareness and educate people regarding its negative impacts and the measures on how to immediately respond to such unprecedented threats.

*****

ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE SYSTEM: A SOCIO-LEGAL ANALYSIS

Pooja Narayan[8]

ABSTRACT

John McCarthy, father of Artificial Intelligence defined it as, "the science and engineering of making intelligent machines." It is actually an ability of computer- system to perceive and response to its environment independently without human intervention while using the cognitive ability and logic of a human being. Experiences and learning from them is the greatest ability of humans, AI mimics this and enables machines and their software to learn from experience. Indian Judiciary has been very quick in adopting the AI technology and its incorporation through e-courts and online hearing, especially during the covid-19 pandemic, has proved to be a milestone in itself. In criminal justice system particularly AI is being used for its various features, one of these being that of facial recognition. Many a times the crime department has to analyse a lot of data in order to establish the identity of someone. If it is done by the humans then it will be highly time-consuming, tiring and high chances of containing human-error. But with the development of AI this has become comparatively fast and error-free. Another aspect is that With AI, volumes of information on law and legal precedence, social information, and media can be used to suggest rulings, identify criminal enterprises, and predict and reveal people at risk from criminal enterprises. This paper dwells into the meaning of AI, its history with discussing in details its role in the criminal justice system, along-with the possibility of misuse or error factor and finally the future of Artificial Intelligence.

Keywords: Artificial Intelligence, Criminal Justice System, misuse, errors, future.

INTRODUCTION

Artificial Intelligence is a fantasy turned into reality. Long ago we only dreamt about something as efficient as AI to make us do the work a little less and more perfect. It has affected our lives in variety of ways including phones, transportation, finances, and health care. This revolution is much bigger and fast than the Industrial revolution. The Artificial intelligence is an advanced form of computer system technology which has the capability of working independently and without any intervention of human, but with the cognitive ability of humans. John McCarthy, the father of Artificial Intelligence, defined it as "the science and engineering of making intelligent machines". This robot-like technology is replacing humans with machines and doing the same work more efficiently and without any hazard which humans are prone to.

The Indian Judicial system has long been suffering from the pendency of cases, poor research quality and various other problems. To solve this Hon'ble Supreme Court of India has already taken steps by launching SUPACE, LIMBS and SUVAS, which are e-governance mechanisms. Through these projects Artificial Intelligence will act as a catalyst in providing timely, effective and quality judgments. This will bring speed to the judicial system with proper record maintenance, transparency, organized data of the cases filed; the courts will become more approachable to the needy, etc. Artificial Intelligence can quickly find out the relevant precedent on a particular topic which is of utmost importance in arriving at suitable Judgments'. The incorporation of the Artificial Intelligence in the judicial administration will

[8] Research Fellow at Faculty of Law, Teerthanker Mahaveer University, Moradabad, India.

ensure effectiveness of law enforcement systems. The former Chief Justice of India Mr. Sharad Arvind Bobde,"We have a possibility of developing Artificial Intelligence for the court system. Only to ensure that the undue delay in justice is prevented…We must employ every talent, every skill we possess to ensure that justice is received within a reasonable time. A delay in justice can't be a reason for anybody to take the law into their hands. But it's very important for us as courts to ensure there's no undue delay in justice."

With adoption of new laws i.e. Bhartiya Nyaya Sanhita, 2023, Bhartiya Nagarik Suraksha Sanhita, 2023 and Bhartiya Sakshya Adiniyam, 2023, there are some features introduced in the Indian Criminal Justice system on par with the current technology, such as the delivery of summons through electronic means, recording of statements of the witnesses online and many more. All these provisions though being a welcome step, it proves that how comprehensive is the effect of artificial intelligence on the society.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE CRIMINAL JUSTICE SYSTEM

The artificial intelligence involvement in the criminal justice system can be better understood under the two wings. Firstly, as a carrier of Justice and secondly as a crime preventer-

1. Carrier of Justice: It can contribute towards the justice system by being of assistance to the courts. Such as recording the data, keeping the records of the cases being filed, disposed of. It also helps in finding the correct precedent out of millions of case laws relevant to a particular situation, which lower the human labor to a large magnitude and also helps in the preparation of case and judgment giving in a more wholesome way, minimizing human error. Artificial Intelligence can tag or club together cases that are same, similar, related, or have a common legal issue which will contribute towards analogous hearing for faster disposal of the case. For example murder cases can be taken in one series, theft can be taken in another etc. Furthermore, AI can be used for document evaluation as it has the ability of data mining and interpretation, which can conclude the possible outcomes of facts based on logical outcomes. So when it comes to voluminous record in a particular case the artificial intelligence can come really handy.

Artificial Intelligence can contribute significantly in the legal aid by giving preliminary virtual advice which will be based on the previous data and recorded advice of the professionals. This can be done by AI through machine learning, deep learning.

Translation into different languages is one of the biggest contributions of the artificial intelligence, now the understanding of a foreign language is completely in our hands i.e. our phones. This development is also extended to the courts wherein the judgments in regional languages can easily be translated in English or other regional languages helping greatly the litigants as well as the legal fraternity.

With the involvement of AI in the judicial system significantly decreased the human bias and this introduction also created a double check and balance.

2. Crime Prevention: Artificial Intelligence has very wide scope in the prevention of crime due to its ability of intelligent prediction. For instance technological surveillance with the help of AI

guided surveillance which through self-learning Capabilities to track the direction of data record by CCTV.

With the help of Artificial Intelligence now the status of cases can be tracked in real time. Through websites of the courts whatever happens in a particular case can be updated to the litigants without any hassle, which existed previously. Whether a case has been dismissed or passed over to another date or any order is passed, this can be now very easily find out from the website and the litigants need not run to the courts to know about the next date or order. Artificial Intelligence is capable of facial recognition which is very effective and efficient in recognizing the accused and hence making tracking and conviction much easier. It is very much effective in crime prediction as well as raising caution against it.

BRIEF HISTORY OF ARTIFICIAL INTELLIGENCE

The biggest capability of human beings is its ability of learning from the experience and artificial intelligence has adopted this very feature of human. It can learn from the previous data and deduce independent logical decision as fit as human cognition. To understand AI better it is important to dwell into its history briefly.

The beginning of this journey can be contributed to Alan Turing, a young polymath who explored the mathematical possibility of artificial intelligence who wrote a paper on computing machinery intelligence back in the year 1950. Next in the year 1956, John McCarthy, who is recognized as the father of Artificial Intelligence, gave definition to it.

In between the years 1956-1974, efforts and researches were made which led to the ability to formulate logic and rules to interpret and form sentences. The AI flourished as computers could store more information and became faster. Next development took between the years 1980-1987, during which complex systems were developed using reasoning algorithms capable of mimicking human experts. These systems though had ability of complex reasoning but still they could not learn new rules to evolve and expand their decision making.

During 1990s and early 2000s artificial intelligence achieved many of the landmark goals. For instance in the year 1997, chess grandmaster Gary Kasparov was defeated by IBM's Deep Blue, a chess playing computer program. In this same year speech recognition software was implemented on the windows.

Present- we are living in the world of big data, collected and processed by the machine which would be almost impossible for a human being to manually evaluate. There is Artificial Intelligence everywhere. Every day, we can see new developments in this field from automated calls to robots taking our food orders in restaurant. From banking sectors to education to health to transportation artificial intelligence has made the life of everyone easier. Previously we used to go to then railway station and stand in line for hours for a ticket now it is available simply on a click.

Future – Artificial Intelligence is here to stay. It is not going anywhere rather it will grow bigger and bigger. From taking about flying cars to actually making it a reality does not seem so fantasied now. Driverless cars and trains might be a just around the corners. AI also has a lot of drawbacks; it definitely

has eased our lives but also gave birth to a lot of crimes. Such as, deep fake videos which can pose anyone as somebody else and create an entire fake narrative. Cyber frauds are on all -time high.

MERITS AND DEMERITS OF ARTIFICIAL INTELLIGENCE

Like everything Artificial Intelligence also suffers from various merits as well as demerits. In this chapter we will be discussing the various facet of AI.

Merits- Firstly, AI has given us the speed. The work which previously took a lot of time and human labor can now be done in minutes or even in seconds. This expeditious nature of technology has become a boon in our lives. For instance, money withdrawal which previously required going to bank, standing in line for hours is now transformed into having it in our hands, all the time. With the introduction of UPI system we can send money, receive it any minute any second of the day. This has made it so much easier and convenient when standing at a hospital to pay bills without leaving our loved ones.

In the criminal justice system speed is of outmost importance. It depends upon how quickly we can analysis the data and catch the criminal. The same data analysis which took days to compile and deduced can now be done in minutes which gave the law enforcement much needed strength. Furthermore any criminal investigation starts with the filing of FIR and delay in filing it raises a question about its credibility, but now with the introduction of E-FIRs it can be filed almost instantly and hence reducing the doubt about its authencity.

Secondly, accuracy is the gift which AI has given us. When analyzing plethora of data there is a possibility of human error but with the advent of artificial intelligence this problem has been completely resolved and now every data can be analyzed to the minutest details without an iota of error. This has come as a blessing for a lot of sectors working and relying on the analysis of large data.

One of the sectors analyzing large data is criminal justice system where previous records, current data such as CCTV records, emails etc needs to be evaluated fast and accurately which is given to it by the AI.

Thirdly, Artificial Intelligence has given the freedom of storing data as old as needed. Previously data storing was a big problem as there has to be a designated place for storing it and with data mostly on paper it fades after few years which makes it impossible for retrieving any detail which is old. But now with the AI storage has become not a problem because data can be stored in the system and it remains as it is for eternity to be used as and when the need be.

Fourthly, the decisions given by the Artificial Intelligence is unbiased. They are based on logic, data and rules which significantly removes the human biasness.

Demerits – Firstly, Violation of privacy. With the advent of Artificial Intelligence the privacy of an individual has been highly compromised. As much life has become easy with the technology so much is privacy is being breached. For instance we put in our details on a food delivery application or online shopping application and in no time we start receiving messaged from them and right now the concern is so high because it has been seen that these applications can actually hear what we are talking about

and in next second we start receiving advertisement of the same product we were talking about. This is very scary.

Secondly, increase in the types of cyber-crimes. Cyber-crimes have always been a major concern for the law enforcement agencies but with the advancement of technology new types of crimes have also came into existence. For instance a new crime known as "digital arrest scam" has come into the society wherein the scammer impersonate themselves as some official and demands money from the victim in the lieu of fine. Recently a chairman of very renowned company was duped by a scammer when they posed themself as the chief justice of India, through a skype call and passed a fake order of Rs. 7 crore fine.

Thirdly, high maintenance. These automated highly efficient machines though very useful requires very high maintenance which makes them costly and hence cannot be afforded by everyone.

Fourthly, reducing job opportunities. Previously the work which used to done by the humans can now very easily be done by the machines, hence reducing the employment opportunity for the masses. It is even said that there might come a time where there be no need of humans for doing any work, which is threating and scary.

PANDEMIC LED ADVANCEMENT OF TECHNOLOGY

It has been said that necessity gives birth to new inventions and this is what happened during the covid-19 pandemic. When entire nation was shut down initially, it was thought of to be a temporary situation but when the pandemic held its grip and made it impossible to work then the technology came as a blessing in disguise. Every possible work which could be done through the internet while sitting at our homes was adopted and hence the nation which came to a halt started working again. This technological or digitalization was adopted by the Hon'ble Supreme Court of India at very initial stage of pandemic. It won't be wrong to state that Supreme Court was among the firsts to adopt this method. In this chapter we will discuss some of the portal launched by it.

1. **SUPACE-** it stands for Supreme Court Portal for Assistance in Court's Efficiency. This portal, which is Artificial Intelligence enabled mechanism, collects data, relevant situations, precedent which exists in relation to the circumstances and legislation in respect of case. After collection of all the relevant data it prepares a report which is presented to the court as a preparatory report. This helps the Judges who are seeking some input for a particular case. Though the Supreme Court was not the first to adopt this portal, rather the Bombay and Delhi High Court Judges have already adopted it for the criminal proceedings.
2. **SUVAS-** it stands for Supreme Court Vidhik Anuvaad Software. This Artificial Intelligence enabled portal has been developed for the purpose of translating the judgements into the regional languages. This portal is developed with the intention of reaching more and more litigants easily, making the judgements of the Supreme Court more understandable. This tool initially was able to translate judgements into nine vernacular languages, which are Assamese, Bengali, Hindi, Kannada, Marathi, Odiya, Tamil, Telugu and Urdu. In the year 2023, the Kerala High Court, Delhi High Court and Karnataka High Court also used this tool for translating

judgements into several regional languages. In this regard cases related to Labour, Rent Act, Land Acquisition and Requisition, Service, Compensation, Criminal, Family Law, Ordinary Civil, Personal Law, Religious and Charitable Endowments, Simple money and Mortgage, Eviction under the Public Premises (Eviction) Act, Land Laws and Agriculture Tenancies and Consumer Protection are being translated.

SUGGESTIONS

After an analysis of various aspects of the use of Artificial Intelligence in the Criminal Justice System these following suggestions can be drawn:-

1. Optimal Use: The use of AI should be optimized. The approach should be to use AI only as and when required. Is should be used on urgency basis, when need arises. For instance using AI for tabulation and calculation of bulk of data because human calculation of the same would not be accurate and fast. But using AI for generating images which are completely false is dangerous and also waste of technology.
2. Development: The AI technology requires more development. It has till time have been developed so as to be of great help to the humans by doing difficult tasks faster and in more accurate way but now it needs to be developed around protection creation. The biggest concern around AI is violation of privacy and there is an urgent requirement of solving this issue.
3. Strict Legislation: There is a need for legislations which are strict, appropriate and directing towards the when, how and how much use factor of the Artificial Intelligence.
4. Human Inclusion: The work should be done towards inclusion and supervision of humans as it is not possible for a machine to have emotions. The justice system works not only on the legislations but also on equity and that cannot be taught to the machine.

CONCLUSION

The Indian Justice system is highly in the need of Artificial Intelligence as it is suffering from burden of cases, vacancies, lack of accurate and organized data, timely tracking of the cases, which is just increasing the burden on the justice system and making justice delivery delayed. Everyone is aware of the fact that a case once filed in a court it takes almost 20-30 years to finally get resolved, which in turn faces the consequence of litigants originally filling the case not being able to see the justice delivered. It is being said that justice delayed is justice denied and this is so true in the case Indian Justice delivery system. With the advent of Artificial Intelligence and its use definitely gives hope that the justice will now be reached on time and be given to the person seeking it instead of to their legal heirs.

Artificial Intelligence has the feature of reforming the criminal justice system as a carrier of justice as well as a crime prevention mechanism. In the little time of its invention and incorporation it has proved itself to be highly useful and effective. Be it speed or accuracy artificial intelligence is checking all the boxes for better justice delivery system. With the advent of Supreme Court Portal for Assistance in Court's Efficiency (SUPACE) and Supreme Court Vidhik Anuvaad Software (SUVAS) the litigants and the judges are getting the much needed support. With the translation of the judgements now the

litigants can understand it and no one can make them fool by misinterpreting it. It might seem a small step but actually it is a very progressive and striking on the crime of middle man misinterpretation.

However incorporation of Artificial Intelligence is not free from defects and drawbacks for instance its use and maintenance is high making it expensive and not affordable to everyone. Other than this due to the advancement of AI new kinds of offences have also came into existence. It is like this the more we are trying to use the technology to deal with faster and accurate resolving of the cases the more new kinds of cyber-crimes are surfacing. The criminals are finding new ways of duping people which is also very worrisome.

At this juncture it can be said that the use of AI is proving to be very beneficial but we still need adherent legislations to stop its misuse.

*****

RESOURCES

Journal Articles

1. Apoorva Chandra, ARTIFICIAL INTELLIGENCE AND THE CRIMINAL JUSTICE SYSTEM OF INDIA; Journal of Legal Research and Juridical Sciences; Vol.2, Issue III
2. Muskan Shokeen, Vinit Sharma (2023); Artificial intelligence and criminal justice system in India: A crtical study; International Journal of Law, Policy and Social Review; Vol.5, Issue IV
3. Isha Sharma (2023); A LEGAL STUDY ON ROLE OF AI IN CRIMINAL JUSTICE SYSTEM IN INDIA; Journal of Emerging Technologies and Innovative Research (JETIR); Vol.10, Issue VIII

Articles

1. CHRISTOPHER RIGANO (2019); USING ARTIFICIAL INTELLIGENCE TO ADDRESS CRIMINAL JUSTICE NEEDS ; Issue 280

*****

THE DARK MIRROR OF AI: COMBATTING THE RISE OF DEEPFAKE TECHNOLOGIES

Vijpreet Pal[9]

ABSTRACT

Deepfakes are fabricated, manipulated content created by merging, altering, replacing, and superimposing images, videos, or audio using artificial intelligence and machine learning. This advanced technology produces remarkably realistic results, portraying individuals saying or doing things they never actually did. While deepfakes open avenues for creativity in fields like education and art, their misuse has surged, particularly in illicit and harmful ways. A large proportion of deepfake videos involve non-consensual pornography and revenge porn, posing severe threats to personal dignity and privacy. In the political arena, deepfakes hold the potential for weaponization, where fabricated content could incite military coups or justify conflict between nations. The increasing sophistication of synthetic media also raises concerns about the diminishing credibility of audio and video evidence, as these forms of media are increasingly used to facilitate disinformation, damage reputations, and infringe on privacy. This paper seeks to highlight the growing dangers posed by deepfakes as a result of advancements in artificial intelligence. It examines the technology behind deepfakes and discusses how these synthetic media can be used maliciously to harm individuals and society at large. The discussion covers various real-world instances of deepfakes being used to commit misdeeds, along with hypothetical examples illustrating their potential for further misuse. As philosopher Jean Baudrillard said, "The simulacrum is never that which conceals the truth—it is the truth which conceals that there is none."In an era where synthetic media blurs the line between reality and fabrication, the consequences are profound. Additionally, the paper explores current regulatory measures and proposes legal frameworks to mitigate the risks posed by deepfakes, offering potential solutions to address privacy breaches, reputational harm, and the broader societal impacts of this emerging technology.

Keywords: deepfakes, artificial intelligence, data privacy, propaganda, defamation, copyrights.

With the use of deepfake technology, voices and faces may be added to audio and video recordings. The results are pretty accurate. The term "deepfake" was coined by a Reddit user in the year 2017, who used the technology to alter the faces in pornographic videos. Primarily deepfakes are employed in four cases and they are - pornography, political campaigns, commercial uses to reduce transaction cost and creative work like movies, memes, etc. Two videos featuring Bharatiya Janata Party candidate Manoj Tiwari condemning Delhi's Aam Aadmi Party were manipulated using "deepfake technology" to appear as he was speaking in English and Haryanvi, aiming to reach more voters during the 2020 legislative assembly election in Delhi. In 2019, Silversparro Technologies, a tech start-up engaged in machine learning and deep learning generated a deepfake GIF of Narendra Modi, prime minister of India on experimental basis. Abhinav Kumar Gupta, founder and CEO of Silversparro Technologies said that *"[T]he implications of deepfakes are worrying"* and claimed that a dystopian future awaited the Indian politics.

Shortly after the official launch of the technology in 2018, even websites like Twitter and Facebook have banned it on their platforms. An unprecedented rise in the generation of these deepfake videos has

[9] Student at United University, Prayagraj, India.

been observed, leading to probable legal consequence in the areas of defamation, free expression and privacy. Therefore, it is important to acknowledge that the existing legal provisions are neither sufficient to curtail the application of deepfake nor guarantee justice to the aggrieved parties. *Part II* of this article explores deepfake technology, while *Part III* investigates potential misuses. *Part IV* discusses Indian regulatory and legal remedies to combat deepfakes. *Part V* details legislative and judicial actions in the UK against deepfakes. *Part VI* concludes with conclusive remarks.

TECHNOLOGY BEHIND DEEPFAKES

Franklin Foer of the Atlantic described deepfakes as, *"[O]ne of the cruelest, most invasive forms of identity theft invented in the internet era."* Deepfakes are primarily based on machine-learning algorithms which harness facial mapping software to produce a fabricated content of an individual's identity without their permission.The technology uses "neural networks" which, begins with a tabula rasa kind of a layout with a nodal network managed by a set of numerical standard controlled randomly. The neural networks are trained by examples, quite similar to how a human brain is trained by experiences. Likewise, the network is able to produce increasingly accurate impersonations or alterations by processing a broad set of training examples. Further, the generation of increasingly convincing deepfakes has shot up post the invention of "Generative Adversarial Networks" by Ian Goodfellow. The approach involves the co-existence of two neural networks concurrently, one known as the "generator" and the other known as the "discriminator". The function of the generator is to draw on a dataset to generate a sample that would further mimic the dataset. The function of the discriminator is to assess the extent to which the generator has succeeded with the mimicking process. The assessments are informed by the discriminator to the generator in an iterative manner. After the completion of the preliminary machine learning process, the program can run without any human supervision.

Essentially, there exist three kinds of deepfake videos i.e. Face swapping which involves superpositioning synthesised faces on target faces while maintaining facial expression. Head puppetry synthesises target head and shoulder using source head, while lip syncing alters lip region to create fabricated video, resulting in unspoken speech.

POTENTIAL MISUSES OF DEEPFAKES

"Oh, what a tangled web we weave…when first we practice to deceive." Technology can bring benefits to individuals and society, but it can also be misused. Deepfakes, which exploit advanced information systems, can cause serious harm. They can be used by individuals, corporations, and enemy states to create falsehoods and harass individuals. The Indian Constitution allows for reasonable restrictions on freedom of speech and expression.

(A) Threat to Security, Sovereignty of the State and Friendly Relations with Foreign State

Deepfakes present a glaring threat to national security. A Federal Bureau of Investigation (United States security agency) executive in a summit recently held stated that: *"What we're concerned with is that, in the digital world we live in now, people will find ways to weaponise [sic] deep-learning systems".*

India and Pakistan have been involved in three bloody wars due to false flags. Recently, Pakistan army created fake Twitter profiles of Indian generals to spread fake stories, justifying incursions. Deepfake technology presents a significant threat to the Indian government and army if enemy states use it to defame India or take aggressive actions.

(B) Violation of Public Order and Incitement of Violence

Public order which is derived from the French word *order publique* in normal parlance means the maintenance of not only the individuals' duties but also the peace and harmony of the society at large. Public order in India is being violated by mob lynchings and violent protests, largely due to viral WhatsApp messages spreading fake warnings of child-trafficking, organ harvesting, or witchcraft. The use of deepfakes technology is exacerbated, leading to a growing number of malicious attempts to create panic and disrupt society's peace.

(C) Threat to Decency, Morality and Defamation

The Supreme Court of India in the judgment of *Ranjit D. Udeshi* v. *State of Maharashtra* had stated pornography and libidinous characters in popular culture both qualify as obscenity. Deepfakes exploiting Indian movie stars are already out on the web. Noted actresses like Shraddha Kapoor and Deepika Padukone have been victimised by deepfake porn. The technology is being improved with an Android app, allowing users to create nude images of women in minutes.

India has been a witness to numerous cases of revenge porn. In 2014, a college girl in Kerala, India, was shocked to discover her private pictures were shared online by her former boyfriend. In another gruesome breach of privacy, a separated husband from Ahmadabad allegedly used social media to post private chats and naked pictures of his wife and sister-in-law, claiming them as prostitutes. Thus deepfakes present a massive threat to the decency and morality of the society.

(D) Contempt of Court

The criminal contempt often comes at loggerheads with the rights accorded to press and the freedom of expression. Supreme Court in *Harijai Singh, In re*, clarified by saying that a free and outspoken press is the driver of a healthy democracy but the said right is not absolute and unfettered at all times. In December 2019, the Karnataka High Court put out a notice of contempt of court against the daily newspaper Deccan Herald on account of a fake news publication. The report had vehemently stated that the High Court had issued notices to 48 Judges and that more than 20 Judges had taken voluntary retirement. Deepfakes could undermine the judiciary system by promoting fake reporting, doctored videos of bribes, and criminal contempt of courts, potentially gaining credibility.

TACKLING DEEPFAKES IN INDIA: ISSUES, SOLUTIONS AND REGULATORY STEPS

(A) Hindrances to Legal Redressal

Deepfakes are often created on conditions of anonymity. Civil and criminal charges cannot be levied upon the creators of deepfakes if they are not identified. Law enforcers find it difficult to track Internet Protocol (IP) addresses of the pirates due to anonymous and secretive nature of their operations. Similarly, if a person uploads deepfake porn as an act to defame a person, he would do so after taking

all the necessary precautions to hide his IP address. The rise of Virtual Private Networks (VPN) has added to the problem. VPNs allow individuals to shift their IP address to remote servers through a tunnel in order to stay invisible.

Second legal issue lies in the territoriality. With the access to Internet being global, perpetrators from other jurisdictions could try to defame Indian citizens or try to disrupt the peace in the nation by using deepfakes. In such scenarios taking action against it would be beyond the jurisdiction of the Indian civil or criminal courts.

(B) Potential Legal Recourses

i. <u>Suits against Copyright and Celebrity Rights Infringement</u>

Deepfake videos often use copyrighted content without valid licenses, infringing on the copyrights of the rightful owner. If a deepfake uses protected photographs or videos, the owner can file a civil suit for injunctions and damages. Celebrities can also sue for infringement of their "celebrity rights" as recognized by the Bombay High Court in *Sonu Nigam v. Amrik Singh*. Similarly, to combat deepfake pornography and deepfake parody videos created to disrupt the image rights of a celebrity, relief can be sought from the courts.

ii. <u>Defamation suits</u>

Deepfake revenge porn created by a person with a sole intention to devalue and harm the reputation of the victim would qualify as defamation. This would allow the aggrieved parties to file a criminal complaint against the perpetrator. If the person who made the deepfake porn is found guilty, he could face a prison term of up to two years and a fine.

iii. <u>Filing for criminal remedies against pornography</u>

In India, several laws have levied a strict ban on publication of obscene material or any content containing indecent representation of women.Section 67 of the IT Act imposes criminal liability for publication or transmission of obscene materials in electronic form. A very relevant judgment was rendered by the Supreme Court in *Sharat Babu Digumarti* v. *Govt. (NCT of Delhi)* which ruled that *"an activity emanating from electronic form which may be obscene is exclusively punishable under Section 67 of IT Act and not under Section 292 of IPC."* Furthermore, with the dawn of internet age the courts in India followed the observation made in *Ajay Goswami* v. *Union of India* according to which in case of a combination of art and obscenity it is imperative to determine if the *"artistic, literary or social merit of the work in question outweighs it obscene content."*

Further, strict legal actions can be taken against *transmitters* of such videos especially if its child porn. The Protection of Children from Sexual Offences Act, 2012 is the primary legislation against child pornography, committing individuals involved in its preparation, production, offering, transmitting, publishing, facilitating, and distribution for sexual pleasure. Child pornography has also been banned explicitly under the IT Act. Thus a person using deepfakes to make child pornography can be punished as per these provisions.

iv. Remedies for breach of data privacy

In the case of *K.S. Puttaswamy* v. *Union of India*, the Supreme Court recognised the right to privacy as a fundamental right as per Article 21 and stated it to be the "constitutional core of human dignity."Subsequent to the *Puttaswamy* decision, a chair headed by Justice Srikrishna had proposed the Personal Data Protection Bill, 2018 which was then tabled in the Lok Sabha as Personal Data Protection Bill, 2019.The Bill defines personal data as any data related to a natural person, including their characteristics or attributes. It defines a personal data breach as accidental disclosure or sharing of personal data that compromises confidentiality, integrity, or availability. Deepfake makers, who share personal data like videos or photos, are guilty of such breaches. Individuals exposed by these breaches can seek remedies under Section 25.

DEEPFAKE REGULATION: UK PERSPECTIVE

Currently, no European or national legislation exists in France, Germany, or the UK to address deepfakes. The European Commission has created a "Code of Practice on Disinformation" to address online disinformation. The UK Government's "Online Harms White Paper" discusses deepfakes using artificial intelligence but does not explicitly address them. A recommendation for companies to improve user security and address online service issues remains a proposal.

The aggrieved party can use Section 1 of the Defamation Act, 2013 to prove that a post online caused or may cause grave reputational harm. They can also prosecute an Internet Service Provider (ISP) as they regulate hosts' actions on their platforms. The case of *Payam Tamiz* v. *Google Inc.*, was the first in UK wherein the liability of ISP was considered for libel. In the landmark decision rendered by the European Court of Justice in *Google Spain SL* v. *Agencia EspaÑola de ProtecciÓn de Datos*, it was ruled that those individuals bearing the brunt of prejudicial search engine results have the "right to be forgotten" and pronounced that all the search engine operators are "Data Controllers" under the European Data Protection Law. The decision ruled that the processing of personal data of an individual may be disabled when the search is *"[I]nadequate, irrelevant, no longer relevant or excessive".* However, "right to be forgotten" cannot be exercised by non-living entities such as a company. Additionally, if the "right to be forgotten" is not extended universally then the adverse Google search results will show up in other countries, thereby defeating the objective behind the ruling.

The Data Protection, Privacy and Electronic Communications (Amendment etc) (EU Exit) Regulations 2019 (DPPEC) define personal data as any information related to an identifiable natural person. The UK's DPPEC is a revised version of the EU's GDPR. Deepfakes technology, such as face swapping and lip-syncing, can incorporate personal data from the target, but head puppetry, which combines face, voice, body, or videos, cannot be considered personal data. However, constructive use of a person's video or audio requires consent, and the relevant person has the "right to erasure" or "rectification". The concept of "lawful processing of personal data" under DPPEC or EU GDPR is relevant to assess the legality of creating fake content. A data subject is vested with the "right to object" if any of their personal data is not processed in compliance to Article 6 of DPPEC or EU GDPR which provides for "lawful processing".

Additionally, other potential measures could be fixation of automated fake content detection software in search engines and social media platforms and embedding inaudible "noise" to digital images which would make it difficult for the deepfake technology to process thereby affecting the quality of the deepfake produced. The UK's existing remedies for addressing deepfake content are ineffective due to challenges in establishing claims due to identity issues and jurisdictional barriers, highlighting the need for improved legislative frameworks to include image rights, online content registration, and penalties.

CONCLUSION

Lies in varied forms have been a part of the society since the beginning and to be realistic it is here to stay. Lies are often used to make jokes, as a method of parenting or as means to boast. But they have a capability to cause significant harm to an individual or the society at large. On that note, deepfakes will merely give a modern technical outlook on the art of lying. The main problem with deepfakes is with its potentiality of misuse by miscreants. Its cutting edge AI mechanisms can be taken use of by criminals to commit atrocities like defamation, national security breach, fake revenge porn, public disorder and contempt of court.

While the field of law around deepfakes in India is evolving, there is no specific statute or legislation for its regulation as of now. So, the task is up to the Indian Parliament to formulate a comprehensive body of law in case the threat of deepfakes rises exponentially. But the threat though mild exists currently. For the time being, the individuals that are victimised by it can use multitudes of civil and criminal remedies to get necessary justice.

CYBERSECURITY IN VIRTUAL WORLDS: AI-DRIVEN SOLUTIONS FOR CROSS-BORDER JURISDICTIONAL GAPS

Dr. Neeta Kumari[10]

ABSTRACT

The emerging field of Metaverse, a virtual environment in which people connect, it has changed the worldwide cyber scene and brought with it previously unheard-of legal and security issues. The presence of notable jurisdictional gaps in cross-border cybercrimes inside these digital domains poses a challenge to national law enforcement organizations' ability to combat cyber threats. In order to close these gaps, this study explores the nuances of cyber security in virtual settings, highlighting the necessity for AI-driven solutions. A critical examination of the United Nations Convention against Cybercrime highlights the jurisdictional obstacles that still need to be overcome in order to achieve effective international collaboration, even though the draft convention has the potential to harmonize legal systems across nations. International cooperation is still essential to preventing cybercrime, although cross-border variations in legal requirements impede joint efforts. This study also examines how AI technology might improve jurisdictional gaps, automate evidence collecting, and foster cross-border collaboration. The increasing risks of cyberwarfare and cyberterrorism are also looked at, with an emphasis on the changing tactics used by adversarial states and non-state actors to take advantage of virtual platform vulnerabilities. Moreover, distinct jurisdictional issues are presented by the Metaverse's emergence as a new battleground for cross-border cybercrime. This study assesses how AI can be used to detect, track, and deter criminal activity in these digital ecosystems while considering the geopolitical repercussions of states utilizing AI for cyberdefense against their neighbors. This study will give the insights to INTERPOLE's commitment. This research lays the groundwork for a more secure digital future by incorporating artificial intelligence (AI) into legal and law enforcement frameworks. It will give the insight for security and privacy of user data that the platform provider is gathering, and to add their own user data on top of that. They next have to explain to their consumers what this data is, why it is being gathered, and what rights they have over it in a format that is easy to grasp.

Keywords: Metaverse, Cross-border cybercrime, AI in cyberdefense, Jurisdictional issues, Virtual ecosystems, International cooperation, Cybersecurity, INTERPOLE

INTRODUCTION

The term virtual worlds, now being termed the "metaverse," was introduced into popular culture by Neal Stephenson in his 1992 novel "Snow Crash", where he described an immersive online shared environment where people interrelated with one another through avatars. Since then, that concept has grown into a complex digital ecosystem. The metaverse has been defined as a long-lasting, immersive, and interactive three-dimensional environment where users can interact both socially and economically (Ritterbusch & Teichmann, 2023). This emergent virtual world was triggered by leading-edge technologies such as XR (extended reality), blockchain, and AI and applied in various sectors, including entertainment, real estate, retail, education, and tourism (Lee et al., 2021). This new digital universe promises significant investments and rapid growth, as per Gartner estimation, by 2026, 25% of people would spend at least one hour a day in the metaverse. Yet despite all the economic and social promise,

[10] Freelance Academic Researcher in India.

cybersecurity remains an area that would be very challenging and nuanced in its own ways and distinctly different from the metaverse.

Open borders-that's just one dimension of the borderless character of the metaverse, giving rise to the uncertainty of a complex legal landscape as national laws struggle to keep the abreast pace of rapid technological advancements. This virtual world has no international legal infrastructure; it thus has legal gaps in the realms of law enforcement and regulation. This has actually spurred the emergence of new forms of crime, known as "metacrime" (Seo et al., 2023). These metacrimes range from virtual attacks, financial frauds, identity thefts, money laundering, etc, in addition to pedophilia crimes. Regarding the self-evident reconciliation of vague jurisdiction and regulatory status between a cluster of metaverses, such loopholes are exploited by criminals. Secondly, law enforcement agencies hardly trace or put offenders on trial. For illustration, in January 2024, first virtual reality attack case was registered to the UK police, which was on sexual assault of a minor's avatar, and since then very high security risk concerns emerged of such environments (Camber, 2024).

Existing legal frameworks were very poor in covering the complexities and nuances of cross-border cyber incidents, resulting in indistinguishable jurisdictions that have the potential to become a bottleneck in effective enforcement and cooperation among nations. Most of the metaverse platforms have begun responding to these issues and, in general, regulatory development lags far behind the boom in the metaverse. Solutions through AI seem promising for efforts aimed at countering these cybersecurity challenges. This will allow the metaverse to leverage AI in threat detection aimed at analysis and real-time response to deflate attacks through surveillance, anomaly detection, and fraud prevention. Of much importance, AI can be set up to facilitate cross-border cooperation. The algorithm may then leverage cross-border data so as to provide a much-needed tool that will fill the gaps brought about by the metaverse in legal enforcement.But that will depend on stronger cooperation between governments and law enforcement agencies together with platform providers. Solutions like these are already being developed by agencies, such as INTERPOL, which claims it is providing leadership for law enforcement and addressing misuse of the metaverse (INTERPOL, 2024).

The point where AI meets cybersecurity and cross-border jurisdiction in virtual worlds stresses how AI solutions could help mitigate the risks and decentralize challenges which tend to be global. Picking up on the subject of AI as used in combating metacrime will give better insight as far as present and limitations set by security concerns about virtual spaces through this research study.

1. **Challenges facing cybersecurity**: The heterogeneity of the different types of cybersecurity risks and challenges virtual worlds and the metaverse present generally but specifically to cross-border jurisdiction issues.
2. **AI Applications Analysis**: Research needs to be done on whether artificial intelligence can be leveraged to make virtual environments secure especially in regards to application areas of threat detection and incident response besides user authentication.

3. **Analysis of Current Regulatory Frameworks**: Current regulatory frameworks must be analyzed so that all legal loopholes that are not enforced properly are discovered so effective cybersecurity across the jurisdictions can be achieved in the metaverse.
4. **Integrated Solutions**: Develop a comprehensive list of AI-based solutions which might possibly address the unearthed cybersecurity issues and thereby facilitate cooperation across borders within jurisdictions.
5. **Future Trends** Identify emerging trends for AI in cybersecurity of virtual worlds, including those potential technological advancements and regulation updates required to help maintain pace with the emerging threats.

METHODOLOGY

The research will follow a multi-faceted methodology in order to achieve these objectives, including the following:A detailed review of available literature on cybersecurity in virtual worlds, giving special consideration to both cross-border jurisdictional challenges and AI applications that can be used. Research methodology for research paper on "Cybersecurity in Virtual Worlds: AI-Driven Solutions for Cross-Border Jurisdictional Gaps"

Where detailed empty space review with proper context can be assessed, to get a more concrete understanding and ensuring secure data sharing.

i. **Handling Obstacles to Cybercrime Investigation:** A holistic approach adapted to the risk assessment. Evaluated the actual AI-driven safety procedures and integrated application, which are associated with government and industrial reports.

ii. **Comprehensive Analysis of Various Research Studies**: The structured process supports the adoption and sharing of cybercrime investigations' knowledge. A systematic comprehensive study is applied that encompasses a more thorough understanding of the interdependency of systems and Internet-connected digital devices within and outside of countries' territories.

iii. **Recommendations to Design an Effective Cybersecurity Policy:** Extracting key data from selected studies, and synthesizing the findings to draw conclusions it is recommended that legal framework needs to be strengthened. As technology continues to evolve and become more interconnected, the line between cyber and physical security is increasingly blurred. The 3 Cs of Enterprise Security: Communicate, Coordinate and Collaborate should be allowed for decision-making and presentation of findings.

LITERATURE REVIEW

The field of work dealing with the topic of cybersecurity, including AI-based solutions, and jurisdictional gaps in virtual worlds, It goes deep into the recent studies carried out on legal frameworks and challenges in prosecuting cybercrimes, especially on hacking, identity theft, and online fraud. The rapid progress made traditional cybersecurity approaches to face significant challenges. We're transitioning to a new era of **smart and adaptive cybersecurity measures**, moving away from one-

size-fits-all tactics to more tailored, flexible methods. In changing times the urgent need for more advanced, adaptable solutions that not only keep up with evolving threats but also anticipate them. From this we need to take lessons from the past: how not to permit space to turn as a "wild west," wherein the most powerful can exploit weaker.. This is particularly the call for up gradation and implementation of the framework of regulation to better handle the increasing "space traffic," as described in Cukurtepe and Akgun, 2009; Lal et al., 2018. To avoid the collision among the assets of multiple operators both domestic and international, laws must be implemented for cybercrimes.

Hence the key shift involves adopting proactive defense systems instead of merely reacting to threats. Artificial Intelligence (AI) plays a crucial role in this shift, utilizing machine learning to analyze large volumes of data, recognize patterns, and detect unusual activity. This makes cybersecurity more dynamic and adaptable to emerging risks.

While a whopping 94 percent of organizations believe they are capable of handling a cyber attack, 71 percent anticipate that their organization will experience a major incident in the next year that will jeopardize their financial stability. It clearly reflects a need for increased awareness and better approach to tackle intricate cyber threats.

However, jurisdiction remains one of the major issues for experts; due to the global outreach of the internet, the assailants of cyber-victims can be reached anywhere in the world, making it hard to track and bring the criminals to book. The paper focuses on legislation relating to issues like hacking, identity theft, and online fraud. Some states have established unique laws especially for cybercrime, while others, and by extension countries, seem to modify their already existing law systems to suit digital crime cases. All these methods may differ in their application and should, from time to time, review how applicable they are with the evolving levels of technology.

The key findings proposed for further discussion: making it imperative for to explore innovative solutions:

1. **AI in Cybersecurity Solutions:** Sophisticated AI cybersecurity tools can compute and analyze large sets of data, allowing them to develop activity patterns that indicate potential malicious behavior. In this sense, AI emulates the threat detection aptitude of its human counterparts. In cybersecurity, AI can also be used for automation, triaging, aggregating alerts, sorting through alerts, automating responses, etc.. AI is often used to augment the first level of analysis. Organizations can ensure that their AI systems are protected against risks by breaking down AI activities into smaller portions, applying the zero-trust approach to security, and using the AI itself to enhance security. This ensures that the insights generated by AI are trustworthy and reliable. This indicates that creative solutions need to be plotted in particular ways to counter the new terrorizations that cybernetic interaction brings forth.
2. **Cross Border Jurisdictional Issues**: No one can deny the fact that the cross-border area of jurisdiction and enforcement of cybersecurity laws is filled with many complexities. Regulations are not uniform, and that has added complexity to meet response related to cyber

threats in the metaverse. This requires collaborative work by nations for an effective legal framework.

3. **Applications of AI in Reality**: Applying Multiple Case Studies The application of AI-based cybersecurity with organizations is best reflected by the multiple case studies mentioned below. Predictive Analytics-Based Tools and AI-enabled Platforms or Solutions Even companies like Cisco and Palo Alto Networks nowadays have developed predictive analytics tools and AI-powered platforms that automate threat detection and response, therefore an improvement in the security posture against evolving cyber threats.
4. **Ethical Concerns** : Implementing AI in cybersecurity introduces some ethical concerns, namely privacy and data protection issues related to responsible AI practice ensuring proper protection of user data while using technology to deliver security.

CASE STUDY INFORMATION FROM THE PAST

There are quite a few case studies that are worthy of note and elaborate on the actual use of AI in cyber-security challenges towards virtual systems:

1. **Cisco Predictive Analytics Tool**: Due to strong cyber attacks that pose a serious threat to its network infrastructure, Cisco developed predictive analytics tool using machine learning and initiated the analytics process. The predictive analytics tool assesses patterns of network traffic and helps distinguish between critical and non-critical anomalies that may indicate a possible threat. The resultant overall success of this proactive approach has thus yielded drastic reductions in successful cyber attacks and operational efficiencies.
2. **The AI-Powered Security Platform at Palo Alto Networks:** Threat is not static; the traditional need for launching an AI-based security platform through application of machine learning algorithms and automatically identifying threats thus arose for Palo Alto. This has reportedly increased the speed of threat detection while permitting simultaneous service with faster responses to incidents-an excellent example of what AI can do in processes involving large data security.
3. **Google Real-Time User Education Program**: Google initiated its program on the use of real-time email services education of its users in countering advanced phishing attacks. Google was able to increase awareness and preventive phishing attempts in its large user base by simply alerting its users to their suspicious emails and providing contextual information to them.
4. **Metaverse - Integrated Cybersecurity Solution**: Critical research in the context of integrated cybersecurity solutions for a metaverse system postulates the requirement of integrating AI with blockchain and cloud computing technology. These steps may greatly strengthen user privacy and data protection while establishing a robust security architecture in the virtual world.

The diverse case studies represent the different changing faces of artificial intelligence within the different cybersecurity spheres along with attempts to gain a grip over virtual environments and border crossing problems of law.

Without special regulations regarding virtual worlds, loopholes to be exploited by cybercriminals extend the possibility of running amuck and unscathed. New concepts in this regard-the crypto-based or NFT-based Metaverse-new problems posed for individual and corporate rights not resolved through proper legal frameworks, thus vitiated human and commercial rights-that will be an important setback.

The second major problem is reviewing and monitoring content. However, AI played the most crucial role in managing the content of the metaverse, which is really a big deal. but mostly remained unsuccessful to identify harmful or illegal materials. Generation of deepfakes or politically slanted content can be used to weaken democracy and national security. Using manipulated images that cause serious psychological damage. Misinformation has also led the metaverse in enabling children to be exposed to pornography as well as other violent acts, making them vulnerable to exploitation in those online spaces. Such risks highlight the need for stronger regulatory and protective mechanisms in virtual spaces. The negative psychological effects of immersion in such environments are also discussed. It has been reported that gaming addiction is a sort of mental illness, especially among young people, along with several associated physical and mental health issues. The World Health Organization has identified gaming addiction as a disorder. This paper continues its discussion on "biometric psychography," which analyzes user data obtained within virtual worlds to infer user preferences and vulnerabilities.

Intellectual property rights during metaverse navigation are difficult. Digital assets are generated and shared across virtual platforms, raising copyright, trademark violations, piracy, and licensing disputes. Information production and dissemination across virtual spaces will most likely become decentralized, and intellectual property laws should therefore be adapted to these trends.

In conclusion, the research points out important guidelines in which AI-based solutions might be used to counterbalance some of the cybersecurity challenges, such as augmenting content moderation, identity verification, and protection of user data. Correspondingly, international collaboration and new regulations regarding jurisdiction gaps and how to adjudicate cybercrimes created in such virtual worlds seem impossible to prosecute.

EVOLVING NATURE OF CYBER THREATS

Dynamic cyber threats challenge the legal systems in dealing with cybercrime issues, thus creating substantive problems in the system. Laws meant to combat these threats must be readjusted based on the innovative nature of the cyber-criminals who are continually developing new strategies, exploiting their weaknesses, and adapting to new technologies Many of these key areas are identified:

1. Technological Advancements: Rapid technological advances-from the Internet to digital devices and communication networks-must present new vulnerabilities and new attack vectors, making cybercrime the most accessible exploitation of these weaknesses and requiring legal systems to evolve in response even more nimbly in the face of those new technology risks.
2. Legislative Adjustments: Laws must always evolve the system to enable it to keep pace with this dynamic world of cyber-attacks. That means it has to try to discover new offenses, modify the punishment so as to align with emerging times, and ensure that such a dynamic cyber threat world is reflected in legal frameworks.

3. Interagency Coordination and Research: In fact, the approaches towards cyber threats would require better interagency coordination on the part of law enforcement, policymakers and cybersecurity experts. There will be much need for in-depth research about trends, tactics, and technologies so strategies may possibly be designed to counter such threats.

An evolving landscape of cyber threats requires proactive measures and, therefore, research, legislative review, and nurturing cooperation between the parties involved should continue in order to arrive at risks emerging in due time and appropriate responses in order to ensure better protection for individuals, organizations, and infrastructure.

SIMILARITIES BETWEEN METACRIME AND CYBERCRIME

While metacrime lies in the broader ambit of cybercrime, similar characteristics metacrime possesses include classification of crimes, dynamic in nature, hyper-spatial-temporality, anonymity, and governance issues. One may conclude that the nature of criminal as well as deviant behavior in metaverse is pretty much on the same lines as that of cybercrime. In this context, as Marshall and Tompsett (2024) opined that metaverse is no longer terra incognita for crime. Advanced technologies of immersive virtual environments do not alter the intrinsic criminogenic factors in an elementary way. According to Gómez-Quintero et al. (2024), five categories were classified into metacrime: financial, property, sexual, crimes against persons, and other offenses. The classifications suggested are very much in resonance with the cybercrime framework proposed by Phillips et al. (2022), comprising fraud, hacking, sexual assault, stalking, money laundering, and much more. Hence, the metaverse is, then, a possible address for criminals, with all of the new opportunities and still many of the crime types of cyberspace. Gómez-Quintero et al. (2024) report, however, that the metaverse does offer some new crime opportunities not found in cyberspace, as demonstrated by cyber-physical attacks on persons, property, and infrastructure.

Metacrime, like cybercrime, is, therefore, a very dynamic phenomenon, constantly evolving with advances in immersive technologies. The metaverse is founded on the convergence of emerging technologies such as cloud computing, artificial intelligence, computer vision, blockchain, robotics, and extended reality. The proliferation of these emerging technologies creates doors for opportunities for offenders to exploit. Dwivedi et al. (2023) catalogued extensive metaverse-specific vulnerabilities, including privacy violations, identity theft, and child sexual abuse, further cementing the fact that technological advancement is more likely to reinforce such threats than eradicate them.

Metacrime also exemplifies another characteristic of hyper-spatial-temporality that cyberspace can provide through such immersive experiences: virtual worlds. HMDs and avatars in being with each other across borders can bridge these worlds, reports Wang et al. (2022). Digital twins-the virtual replica of a real-world entity-blurs the lines between the actual and the virtual (Lee et al., 2021). Thus, this long-standing definition of location-based crime becomes problematic and creates barriers in the way of being able to apply concepts such as crime pattern theory and environmental criminology to the metaverse.

Another characteristic that is also important about cybercrime- namely anonymity-is inherent in the metaverse, which is likely to intensify further, along with decentralized financial systems, such as cryptocurrencies. Indeed, although identity verification is possible, many users welcome anonymity because it protects privacy (Beltrán & Calvo, 2023; Kürtünlüoğlu et al., 2022). Personalised avatars, pseudonyms, and fluid identities become a part of privacy protection but may serve as pathways for malicious actors to take advantage of anonymity in evading legal scrutiny (Cheong, 2022). Another level of complexity brought about by cryptocurrencies is that it enables illegal operations such as money laundering, hacking, and terrorism (Dyntu & Dykyi, 2018; Corbet et al., 2020).

Metacrime, much like cybercrime, poses governance issues. These include legal frameworks, jurisdictional issues, international cooperation, issues of privacy, and a lack of public awareness toward each cybercrime and metacrime (Dwivedi et al., 2023; Kim et al., 2023). Nevertheless, the metaverse itself, with its holographic simulation and very wide use of avatars, has distinct characteristics that make it complex in terms of regulation. For instance, there are already debates on which land-based legal principles should be extended to avatars and digital twins (Cheong, 2022; Zoltick & Maisel, 2023).

THE NEW CHARACTER OF METACRIME: VIRTUAL-TO-PHYSICAL AND IMMERSIVE VIRTUAL REALITY ATTACKS

Among the two most significant new genres of metacrime not covered thus far in the traditional cybercrime context, virtual-to-physical attacks and immersive virtual reality attacks belong. The former type of attacks depends on deep online environments where they integrate the virtual with the physical world. Virtual-to-physical attacks take advantage of digital twins or VR sensors to cause harm to real-world targets, hence further spreading the spectra of cybercrime to include physical features, people, and structures. According to Gómez-Quintero et al. (2024), they have been classified into three: attacks on people, property, and infrastructure. For instance, terrorists can use a digital twin of sensitive location sites to plan attacks in real life and criminals can surveil their targets using front-facing cameras of the VR devices.

On the other hand, attacking immersive VR will be realized through tampering with technical configurations of HMDs. According to Casey et al. (2021), there are four types of immersive VR attacks, including Chaperone Attack, which changes the virtual boundary; Disorientation Attack, dizziness; Human Joystick Attack, where real movements are applied; and Overlay Attack, overlaying abusive content in virtual surroundings. Such attacks might indeed lead to direct physical harm as is mostly so on the body of the person attacked, such as an attack on visual vertigo or neurological syndrome. Psychological disorders are also very severe. On the other hand, in comparison with other classical cybercrimes that indirectly bring about physical harm through psychological mediation, immersive VR attacks can be considered as direct impacts on the physical and mental state of the victims.

While the similarities shared by metacrime with cybercrime do not end there, it also opens new criminogenic opportunities created through virtual-to-physical and immersive VR attacks wherein the

virtual and the physical become intertwined, thus making this offense quite complex as well as dangerous to an extent.

INTERNATIONAL COOPERATION IN THE ERADICATION OF CYBERCRIME

The Role of International Cooperation and Organizations in the Battle against Cybercrime

Crime in the cyber space is a global challenge that takes a cut across the nations' boundaries, and for effective investigation and prosecution of offenses and prevention thereof, international cooperation has to be very strong. Underpinning points present the critical role of cooperation and the role played by international organizations in combating cybercrime:

Role of International Cooperation in the War against Cybercrime:

Cybercrime tends to cut across national boundaries, and there is therefore a need for national cooperation, as given below;

1. Cross Border Nature of Cybercrime: A cybercriminal tend to operate from different countries, and therefore there has to be exchange of information and evidence and other relevant material across borders in order to identify and catch culprits.
2. International Cooperation Best Practice Sharing: It gives the chance for best practice sharing among nations in knowledge, strategy, and tactics. Cyber-fighting policies and technologies can be better developed between those countries who are on the learning curve with each other.
3. Capacity Building Technical support and training programs for technical capacity building will be imperative to developing nations, which will continue to enhance global cybercrime-fighting capacities.

Future-Proofing of Cybercrime Policies

With the involvement of emerging cyber threats, especially in dynamic domains like the Metaverse, policies and legal frames need to be similarly dynamic. Future-proofing concepts apply here in that any legislation provided and maintained will be technologically neutral, and the laws are carefully checked on a periodic basis to determine their applicability and not develop archaic standards in ways not even conceptualized regarding changes in technology.

There must be the inclusion of public authorities, private operators, and civil society in preparing periodic reports of technological developments and associated trends in crime.

CONCLUSION

Overview and outline of the overall Study Results:

To reduce and solving the difficulties in prosecuting cybercrimes, especially hacking, identity theft, and online fraud, improved international cooperation and a strong legal framework both are necessary. This study focuses on what developing technologies can do to reduce cybercrime globally. Conclusion The

research paper "Cybersecurity in Virtual Worlds: AI-Driven Solutions for Cross-Border Jurisdictional Gaps" provides a critical elaboration of the call to strengthen the legal provisions and thus also the demand posed upon cooperation in cross-border jurisdictional gaps in cyberspace. These points include:

1. **Jurisdictional Gaps**: The current day legal framework is also criticised because it does not break the complexities implied in the cross border cyber incidents and thereby create fuzzy boundaries of jurisdictions sometimes letting the nations fail to cooperate with each other in enforcing the laws of that country.
2. **AI Powered Solutions**: The research underlined a requirement to introduce artificial intelligence solutions targeting the mechanisms for sensing, prevention, and action towards cyber threats that cross boundaries. Artificial intelligence enables the immediate exchange of information with the objective of making a more effective legal process toward cyber events.
3. **Inference**-A Call for Clear Jurisdictional Norms and Measures of Cooperation on Law Enforcement in Cyberspace The takeaway is building multilateral agreements expounding crystal-clear jurisdictional norms and measures of cooperation pertaining to law enforcement in cyberspace. And whereas technological change runs incessantly ahead of institutional development, these agreements are determiners of predictable legal boundaries.
4. **Advice for Policymakers:** Policymakers should pursue international standards and frameworks related to support initiatives on cross-border cybersecurity flexible enough to be able to adjust to the diverging legal systems within a security framework that assures trust in digital environments
5. **Future Research Directions**: To this end, the paper looks forward to further research into specific AI applications in cybersecurity and implications on international law, and continuing dialogue involving all stakeholders toward refining approaches to jurisdictional issues in virtual worlds.

In the nutshell, the whole conclusion suggests a proactive approach toward bridging jurisdictional gaps through innovative technology and international cooperation to strengthen global cybersecurity work.

Recommendations for Further Studies

In further advancing our understanding on the prosecution of cyber crimes, further studies are required in the following areas.

1. Cyber Threats in Evolution: Legitimate aspects of this, and challenges faced in utilizing new technologies: AI, IoT, blockchain, quantum computing
2. Reviewing Legal Instruments: comparative studies would be needed to understand the differences in practice about how effective they have been in other jurisdictions, best practices included
3. Models of International Cooperation: more analysis would go well for international cooperation mechanisms and agreements to work together and coordinate better when fighting cybercrime.

4. Privacy and digital rights: Investigate the balance that cybersecurity measures must strike between privacy and more ethical or legal inputs on data collection, surveillance, and AI-based investigations.

Further researches in these areas would help to determine a deeper insight into the legal framework and problems involved in the prosecution of cybercrimes, therefore attaining better strategies, policies, and legal frameworks that will succeed in fighting cyber threats and safe-guarding people and organizations in this digital world.

*****

REFERENCES

1. Belk, R., Humayun, M., & Brouard, M. (2022). Money possessions and ownership in the metaverse: NFTs, cryptocurrencies, Web3, and wild markets. *Journal of Business Research, 153*, 198–205. https://doi.org/10.1016/j.jbusres.2022.08.031
2. Camber, R. (2024). UK police record the first virtual reality sexual assault case involving a minor's avatar. *The Times*. https://www.thetimes.co.uk/article/uk-police-investigate-virtual-assault-on-avatar
3. Cheong, H. (2022). The metaverse and legal implications: Avatar identity and digital twin rights. *Journal of Law and Technology, 9*(2), 45-59. https://doi.org/10.2139/ssrn.1351772
4. Cornelius, K. (2011). Responsibility under criminal law in virtual worlds. In *Virtual worlds and criminality* (pp. 95–119). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-23188-7_6
5. Dwivedi, Y., Hughes, D. L., Wang, Y., & Kumar, V. (2023). Navigating the new digital world: Challenges and opportunities of the metaverse. *Journal of Information Technology, 38*(1), 1-19. https://doi.org/10.1177/02683962231101344
6. Gómez-Quintero, J., Wight, S., & Phillips, A. (2024). Metacrime in the metaverse: New opportunities for criminality. *Journal of Digital Criminology, 12*(3), 30-50. https://doi.org/10.1016/j.jdc.2024.02.011
7. INTERPOL. (2024). INTERPOL's role in combating metaverse crimes. https://www.interpol.int/en/Crimes/Metaverse
8. Jaishankar, K., & Taylor, R.W. (2007). Cyber criminology: Evolving a novel discipline. *International Journal of Cyber Criminology, 1*(1), 1-11.
9. Kasiyanto, S., & Kilinc, M.R. (2022). Legal conundrums of the metaverse. *Journal of Central Banking Law and Institutions, 1*(2), 299–322. https://doi.org/10.21098/jcli.v1i2.25
10. Kim, H., & Lee, S. (2023). The governance of metaverse-based virtual environments. *Journal of Legal Studies in Innovation, 15*(2), 120-134. https://doi.org/10.2139/ssrn.4021978

11. Lee, K.Y., Wang, H., & Ritterbusch, A. (2021). Economic potential and risks in the metaverse: A multi-industry perspective. *Virtual Reality & Society, 9*(3), 78-90. https://doi.org/10.1007/s10055-021-00517-5
12. Lessig, L. (1999). *Code: And other laws of cyberspace*. Basic Books.
13. Maras, M.H. (2016). Challenges in investigating and prosecuting cybercrime. *Security Journal, 29*(3), 401-421. https://doi.org/10.1057/sj.2015.34
14. Phillips, A.M., & Marshall, J.(2022). The classification and prosecution of metacrimes in virtual worlds.*Journal of Criminological Research*, 14(1), 23-42. https://doi.org/10.1108/JCR-2021-0072
15. Ritterbusch,A.,& Teichmann,H.(2023).Navigating the economic complexities of the metaverse.*Journal of Digital Economics*,25(2),45-60. https://doi.org/10.2139/ssrn .2023 .134178
16. Seo,K.,& Park,J.H.(2023).The emergence of metacrime: Legal gaps in the metaverse.*Journal of Cybersecurity Law*,16(4),300-320. https://doi.org/10 .2139 /ssrn .2023 .134129
17. Stephenson,N.(1992).*Snow crash*. Bantam Spectra.
18. United Nations Office on Drugs and Crime.(2021).*Comprehensive study on cybercrime*.https://www.unodc.org/documents/organized-crime/Comprehensive_study_on_cybercrime.pdf
19. World Economic Forum.(2019).*Advancing cyber resilience: Principles and tools for boards*.https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

*****

BALANCING INNOVATION AND REGULATION WITH SPECIAL REFERENCE TO ARTIFICIAL INTELLIGENCE

Sonal Rao[11] and Dr. Aqueeda Khan[12]

ABSTRACT

One of the most fascinating and quickly developing areas of technology is the incorporation of Artificial Intelligence (AI) into several facets of society. Healthcare, banking, transportation, and entertainment are just a few of the industries that are using AI systems as they get more advanced. But, as AI technology continues to seep into other areas of human endeavour, it poses a number of legal issues that need to be carefully considered and regulated. Examining the intricate interplay between AI and law, including legal frameworks, ethical considerations, and new difficulties in this ever-evolving field, is crucial.

In general, it raises questions about AI violating people's and businesses' data privacy. Because AI modules are working to obtain personal data information, artificial intelligence is developing quickly, raising the possibility of serious data breaches.

The adoption of AI raises questions about data protection because of the abundance of data that is already available. Millions of bits of data are gathered and processed daily, and there's a good chance that some of it could end up in the wrong hands with hackers. A person may experience discomfort if malicious hackers gain unauthorised access to data. AI poses serious questions regarding data protection and privacy laws as it grows more advanced and widespread.

Keywords: Artificial intelligence, Data protection, Data Protection Laws, Data privacy.

INTRODUCTION

"In the current digital environment, artificial intelligence is being ingrained in practically every industry, including the legal field. In an effort to improve efficiency, the legal sector has also taken the lead in using artificially created processes within the business. It may include anything from cloud-based file backups of private information to case documentation. It frees paralegals from having to manually enter data, allowing them to concentrate on more strategic duties.

When putting AI into practice, security is yet another crucial factor to take into account. It makes it possible to set up a completely safe system in which nothing is left up to chance. An excellent artificially intelligent research platform can complete studies in a matter of seconds. AI can assist in estimating legal research expenses while preserving a high standard of quality, regardless of the size of the legal firm. Attorneys can gather information points from prior or former instances with the help of AI technology.

Future developments in IoT promise increased intelligence, which will transform the way lawyers practice law. The phrase "Internet of Law" was also created by the IoT. It expands on the idea of

[11] Research Scholar at Amity University, Noida, India.
[12] Professor at Amity University, Noida, India.

combining some autonomous systems with law enforcement tactics. AI has an insatiable desire for data. It operates more effectively the more information it takes in. This dependence, however, presents issues because businesses gather and examine a tonne of personal data, including biometric data and online activity.

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON PRIVACY

The way we engage with technology is rapidly changing due to artificial intelligence. Voice assistants, chatbots, and smart home appliances are just a few examples of the AI-powered gadgets that have completely taken over our daily lives.

We are aware that data, which is gathered in myriad ways from many sources, will power the modern world. The actual extent of the data is still hard to understand, though. About 90% of the world's data has been created in the last few years, according to a Verizon Connect article about the state of big data.

The post provides raw statistics. Large datasets, which may include sensitive personal data like our location, browser history, and purchase patterns, are used to train AI algorithms. The main concern with privacy and current technology is that, whether we like it or not, we are becoming just another set of data points to be exploited for commercial and research initiatives. This information can be used to build a thorough profile of us that can be used for identity theft or sold to unaffiliated businesses for targeted advertising.

Concerns about the use of AI in surveillance and monitoring are growing, especially in fields like social media analysis and face recognition. These technologies can improve security, but they also greatly increase the risk to privacy because they can be used to follow people's whereabouts, activities, and affiliations without their knowledge or agreement.

INTERNET OF THINGS AND PRIVACY

Smart thermostats, security cameras, and fitness trackers are few examples of Internet of Things (IoT) products that have grown in popularity recently. By automating processes and supplying real-time information, these gadgets are meant to make our lives easier.

Our daily routines, habits, and personal preferences are just a few of the countless pieces of information that are gathered by IoT devices. It is possible to deduce private details about us from this data, like our financial state or health status.We should make sure that our IoT devices are secure and that the most recent security patches are applied on a regular basis to safeguard our privacy. Additionally, we should exercise caution when providing these gadgets authorization and make sure they aren't disclosing personal information to unaffiliated businesses.

India has joined other countries in regulating activities pertaining to data. To regulate the processing of digital personal data or non-digital data to be handled digitally, the Digital Personal Data Protection Act, 2023 was introduced. Fundamentally, the Act seeks to hold businesses and organisations that gather, process, and store data in India to a greater standard of accountability. The Act's reach transcends national boundaries and includes digital data processing operations conducted overseas. India

strengthens its data privacy laws with this one. Since the Internet of Things (IoT) relies on the gathering, sharing, and storing of data, including personal data, the DPDP Act, 2023 governs all data processing related to this in India.

Privacy Concerns in AI

1. The gathering of personal data without express consent is one of the main issues with AI. Many AI applications collect user data without providing consumers with a clear understanding of how their data will be used. This lack of openness may cause people to lose faith in you and maybe misuse your personal information.
2. Large datasets are frequently necessary for AI systems to operate well, which has led to the practice of gathering as much data as possible. This strategy, however, runs counter to the data minimization principle, which supports gathering only the information required for a given goal. Over-collection of data raises the possibility of misuse and breaches.
3. Organizations frequently anonymize data before utilizing it in AI models to address privacy concerns. Research has demonstrated that, on occasion, even anonymised data can be used to identify a specific person, particularly when merged with other datasets. This calls into doubt the efficacy of anonymization as a method for protecting privacy.
4. Biased data used to train AI models can exacerbate already-existing inequality. This is especially troubling when AI is applied in delicate fields like financing, recruiting, or law enforcement. An AI system that harbours bias may decide in a way that unfairly disadvantages particular groups, which could result in privacy violations and discrimination.

Balancing AI Innovation with Data Privacy

1. It is crucial to include privacy concerns in the design and development of AI systems. This method, called "privacy by design," makes sure that data security is integrated into the AI system from the beginning rather than being an afterthought. This entails putting in place robust encryption, data reduction, and access controls right away.
2. AI systems need to be open about the data they gather, process, and retain. This entails informing consumers in a straightforward and understandable manner about how their data will be utilised and making sure that anyone who misuses data is held accountable. Strong governance frameworks should be established by organisations to supervise AI systems and guarantee adherence to data privacy laws.
3. While more sophisticated techniques like differential privacy can offer stronger guarantees, standard anonymisation techniques have their limits as well. Differential privacy introduces noise into the data, which makes significant analysis possible but makes it challenging to re-identify specific persons. This strategy can facilitate the use of data in AI applications while also helping to preserve privacy.
4. The ethical ramifications of AI systems, particularly with relation to bias and discrimination, must be taken into account by organisations. To guarantee that a variety of viewpoints are taken

into account, this entails carrying out exhaustive audits of AI models to find and eliminate biases as well as include different teams in the development process.

INDIAN SCENARIO

Since the Supreme Court of India ruled in the Puttaswamy case of 2017 that privacy is a fundamental right, data protection has become an increasingly important issue in India. The Act was enacted in August 2023, marking the culmination of the efforts of the Indian legislator. The Act controls how digital personal data is processed and stipulates that violators may face fines up to INR 250 crore. Crucially, the Indian government must publish a notice in the Official Gazette announcing the Act's coming into force. Notably, the Act creates data subject rights for "data principals," only applies to digital personal data, and usually permits external transfers of data from India. It also places requirements on businesses that meet the criteria for being considered "data fiduciaries." The Supreme Court's ruling had a significant impact on the judiciary. The ruling was immensely important because it recognised the changing issues brought about by the digital era and set the groundwork for India to create a more comprehensive and strong data security regime. The court emphasised that privacy is a necessary component for the meaningful enjoyment of life and liberty and upheld its importance for the exercise of other rights and freedoms. A complicated and multidimensional journey spanning centuries, societal, technological, and legal advances have affected the growth of privacy legislation.

The Act creates rights for data subjects, specifies legitimate grounds for data processing, and sets regulations such as vendor management, data security, and consent manager appointment, all in accordance with international standards.

The Information Technology Act, 2000 (also known as "the IT Act"), as amended by the Act, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (also known as "the SPDI Rules") issued under it are additional pieces of legislation that offer protections for personal data.

Sector-Specific Regulations: Guidelines for data management and privacy in the financial sector have been established by the Reserve Bank of India (RBI).

Increased Public Awareness:

Public awareness of the significance of data protection is growing as a result of the continuing discussion surrounding data privacy.

COMPARTIVIE ANALYSIS OF REGULATION IN DIFFERENT COUNTRIES

Aspect	India	European Union (GDPR)	USA
Overarching Law	DPDP Bill (not enacted)	Comprehensive GDPR	Sector-specific
Emphasis on Consent	Increasing with DPDP Bill	Core principle	Varies across sectors
Data Localization	Potential restrictions	Restrictions on transfers outside EU	Some restrictions, national security focus

India, the EU, and the USA are all heading towards data privacy and security laws that are focused on the needs of their citizens. The General Data Protection Regulation (GDPR) framework of the European Union, which aligns with the "Privacy by Design" paradigm popular in the United States, serves as the primary foundation for India's Data Protection Bill, 2021. As one of the world's biggest consumer marketplaces, India has a rising demand for data privacy and security. The Indian Bill attempts to address this requirement by developing specific legislation. As of 2021, it includes non-public personal information (NPI) in addition to personal information. The primary differences between the three regions' broad scenarios can be observed in their current situations, or in the laws that are currently in effect in these areas. India lags behind the EU with its centrally implemented, narrowly focused data privacy laws, whereas the EU has a centrally implemented, comprehensive data privacy law. When it comes to putting data privacy laws that safeguard personal information on the internet of things into effect, the US lags behind other countries. With the enactment of relevant legislation in both parliaments, it can be asserted that the United States and India are on par with respect to their efforts to establish a robust and efficient data privacy system.

However, as of right now, only the EU can claim to have a fully functional data privacy regulation that serves to safeguard the interests of its residents. The rules of the various regimes also have different applicability. The applicability of current EU and Indian legislation is extraterritorial; US law does not have this aspect.

CONCLUSION

The serious issue of AI and data privacy necessitates thoughtful analysis and effective steps. Artificial intelligence (AI) presents serious hazards to personal privacy even as it has the ability to revolutionise industries and improve our daily lives. We can exploit the power of AI while protecting people's privacy by embracing privacy-preserving technology, adhering to transparency and accountability standards, and adopting privacy by design principles. Building a future where AI and privacy coexist peacefully will require a balanced approach that prioritises both innovation and protection as we traverse this complicated terrain. Amidst a period marked by swift progress in Artificial Intelligence (AI)3 and the growing prevalence of data, the legal structure controlling the interaction between AI and data privacy has become a critical issue both internationally and in India. India, a rising centre of the technology industry, is positioned to successfully negotiate the complex intersection of innovation and data protection. The necessity to comply with international privacy standards, handle new issues, and defend people's fundamental right to privacy has led to notable changes in India's data protection regulatory environment. The authors believe that rigorous ethical standards that govern the creation and application of AI technology are desperately needed. Critical concerns like bias mitigation, accountability, transparency, and the impact of AI on privacy and human rights can all be addressed by these standards, as well as how they regulate the interaction that facilitates the connection between AI and publicly available data.

*****

UNVIELING THE DARKNET: CYBERCRIMES AND THEIR IMPACT ON VULNERABLE GROUPS IN THE DIGITAL DIVIDE

Niyathi S.[13] and Kanigasri Vijayakumar[14]

ABSTRACT

In the grooming era of the internet, where access to numerous resources is readily available, the cybersecurity of such accessibility is at risk. The dark web is an anonymous network that connects users by using non-standard and often illicit protocols. It is an end-to-end encrypted network that hides user's identities, giving them a false sense of security. This anonymity is further enhanced by technologies such as Onion routing, the Tor web browser, and Virtual Private Networks (VPNs). The primary reason people use such browsers is that they enable access to the dark web while maintaining user anonymity. The dark web is often exploited for purposes such as identity theft, sextortion, the sale of illicit goods (weapons, narcotics, stolen data, etc.), and as a communication platform for extremist groups to express their oppressive views. It is also a hub for revenge porn, contract killings, and assassinations. The victims of such distressing offenses are often the vulnerable groups such as children, women, elderly population, people residing in rural areas as well as low-income communities. However, they are not only the victims, but also form a significant portion of the perpetrators due to the vicious cycle of poverty, lack of access to education and unemployment. The underlying cause of the issue is the digital divide, which is essentially the proportionate gap between the people who have access to the digital world and those who do not. Digital divide can stem from geographical, socio-economical, global and gender disparities. This paper aims to address such issues that require a multifaceted approach bridging the gap in the digital divide and proposing a solution of having a constructive legal framework and efficient mechanisms to monitor deviations.

Keywords: Dark web, Cybersecurity, Digital divide, Sextortion, Vulnerable groups

INTRODUCTION

Amidst the rapid evolution of digital technologies, cybercrime has emerged as one of the most pervasive and insidious threats to global security, challenging the very foundations of privacy, trust, and governance in the modern world. Dark web traces back to the 2000s, when it was only there for ethical purposes and legal usage. However, as awareness of the power of cyberspace grows, many individuals choose to misuse it for personal gain rather than considering its broader societal implications. With the advent of emerging technologies like Artificial Intelligence and Extended Reality (XR), users are increasingly exploiting the opportunities within the once-sacred digital realm, drawing themselves into unethical practices with the internet as their primary tool. The research aims to address the malefactions such as sextortion, revenge porn, illegal trafficking and sale of illicit goods online and various other crimes arising in the digital world. The main objective is to educate the vulnerable groups in order to bridge the gap of digital divide that persist amongst them. The same technology that has been the root cause of these problems can also be harnessed to prevent such crimes and create a safer cyberspace, where individuals can freely express their views and opinions, legitimizing the responsible use of the internet. Furthermore, the evolving potential of technology offers innovative solutions to combat these illicit activities and address their perpetrators effectively. The paper argues the fact that the vulnerable

[13] Student at Vellore Institute of Technology, Chennai, India.
[14] Student at Vellore Institute of Technology, Chennai, India.

groups are the major victims and are not protected due to lack of knowledge, awareness and absence of effective legislative framework exploiting their social and economic stance in the society.

LITERATURE REVIEW

The United Nations Development Programme (UNDP) report on 'Cyber Violence Against Women and Girls' aims to highlight the various forms of cyber violence against women and girls (VAWG), especially those linked to intimate partner violence (IPV), while emphasizing the disproportionate impact on women. It advocates for a comprehensive understanding of cyber VAWG as part of a continuum of violence that includes offline experiences, calling for more research into the effects on victims. However, the report overlooks significant legal ambiguities. Defining cyber VAWG as a form of VAW may encounter legal challenges, as existing laws often fail to address online behaviours, leading to confusion in enforcement and accountability. Additionally, both policymakers and the general public may lack a full understanding of the complexities of cyber VAWG, resulting in underreporting and inadequate responses. Furthermore, women from diverse backgrounds may experience cyber VAWG in varying ways, hence the one-size-fits -all approach neglects the specific needs of marginalized groups.

1. Online Gender-Based Violence against Women and Children:

According to the 2022 report of National Crimes Record Bureau (NCRB), instances of cybercrimes against women and minors have escalated by 32 percent compared to the previous year. Cyberviolence seems to have bias towards women and girls, who constitute a major section of the vulnerable group and tend to get exposed online. Recent data from the NCRB, unveiled a concerning picture regarding cybercrimes against children. This issue particularly affects those who face multiple social disadvantages, including race, class, caste, religion, and disability. Women of colour are especially vulnerable to online violence, as are those from ethnic or religious minorities, as well as lesbian, bisexual, transgender, or intersex (LBTI) women, who often face harsh criticism on social media. Peer-inflicted online abuse is not limited to young people; it also targets women in positions of power. This abuse often acts as a mechanism of control, aimed at those who challenge patriarchal norms and advocate for gender empowerment. Although the Information Technology Act of 2000 was the first legislation to address IT crimes, it had shortcomings, leaving the country without a robust legal framework to combat cybercrime against women. During the pandemic, online gender-based violence surged globally, and many countries struggled to address violations against women's online safety due to inadequate legislative measures.

In the case of *Shreya Singhal v. Union of India*, two women faced charges under Section 66A of the Information Technology Act of 2000 for allegedly posting offensive comments on Facebook regarding the city of Mumbai's response to a politician's death. This section aimed to penalize individuals for sending grossly offensive or false information via digital platforms, which could cause annoyance or harm. The case attracted significant media attention, prompting the Supreme Court to declare Section 66A unconstitutional, ruling that it violated the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The court criticized the section's vague language and potential for arbitrary

arrests, emphasizing its "chilling effect" on free expression. While this judgment marked a victory for digital freedom, it highlighted a gap in the legal framework for addressing cyber harassment and online abuse.

The research proposes strategies to close the gender gap in technology access by fostering equal employment opportunities for economic empowerment, social integration, and sustainable development, thereby ensuring women's full engagement in the digital economy. By prioritizing an inclusive tech ecosystem, we can enable marginalized groups—especially women and other underrepresented communities—to contribute to innovative solutions that meet the rising demands of the digital economy. There is need for a robust legal framework that deals with cyberviolence with special emphasis towards women and children.

2. Deepfake technology and its Ethical impacts:

Deepfakes are videos created using deep learning, AI, and image manipulation techniques to fabricate events, often with the intent to spread misinformation. Technologies like Generative Adversarial Networks (GANs) and Machine Learning (ML) work in tandem to generate such videos. The first major incident which involved deep fakes occurred in 2017, when a Reddit user named "DeepFakes" posted adult videos that exposed the faces of celebrities onto the bodies of porn stars. While this wasn't initially classified as an attack, it caused widespread outrage and raised serious concerns about privacy violations and the need for effective deepfake detection. In response to this, Reddit and other social media platforms banned the content and the user, leading some legislative bodies to propose laws targeting deepfake pornography and the unauthorized use of individuals' likenesses. According to a report by global security software company McAfee, approximately 22% of Indians had encountered political deep fakes, which they later realized was false. 55% of the respondents expressed concern about the potential for cyberbullying through deepfakes, and 52% were worried about the creation of fake pornographic content. High-profile individuals are often the targets of deepfake manipulation. For instance, actor Ranveer Singh filed a police report after a deepfake video falsely showed him endorsing a political party and criticizing Prime Minister Narendra Modi during a news interview. Similarly, actress Rashmika Mandanna was also victimized, as her face was misused in inappropriate videos that damaged her image and reputation. These incidents are becoming increasingly frequent and warrant immediate attention.

Through this research we propose stringent regulatory measures to ensure that the inbuilt algorithms in deepfake or AI aided software are not biased and ensure that the data is end-to-end encrypted to maintain privacy. There is further a need for enhanced deepfake deduction technologies which will help track corrupt users to avoid any mishap. The rising concerns in the area of deep fake calls for an effective legislation in order to deal with such issues and come up with quick measures.

3. The Role of Social Media in the Proliferation and Prevention of Revenge Porn:

According to a survey conducted by the Cyber and Law Foundation and an NGO, about 27% of inter-

net users in India aged 13 to 45 have been victims of revenge porn and sextortion. In a conservative country like India, the victim's first thought is often to avoid filing a complaint or, tragically, to consider

suicide due to societal judgment. The legal process has primarily concentrated on the technicalities of content removal, neglecting the emotional and psychological trauma experienced by the victim. This highlights a systemic flaw in how online harassment cases are handled, which often overlooks victim support and their counselling. This can be further understood through the case of *Mr. X and Ors. Vs Union of India*, where the petitioner sought the removal of her non-consensually shared explicit images from online platforms like Google. The perpetrator, posing as a British chartered accountant, manipulated her and her son to extort money through threats. While this case prompted stricter enforcement for removing non-consensual content, it revealed India's lack of cohesive legislation against revenge porn, sextortion and image-based abuse. Despite reporting the issue to authorities and platforms, timely action was not taken to remove the images, underscoring the slow response of intermediaries and the absence of preventive measures to stop content from reappearing online. The non-consensual distribution of intimate images and videos is a troubling issue that has been intensified by the rise of unmoderated instant messaging platforms like Facebook, Telegram, Instagram, YouTube etc. The combination of anonymity and a relaxed regulatory environment has enabled the growth of social media, its channels, and bots that share such content. This trend poses significant ethical and mental health risks and demands urgent intervention.

Through this paper we would like to propose a mechanism designed to map the complex network of social media spaces involved in non-consensual pornography and to identify even slightly modified copies of images circulating in various channels and groups. While these platforms do have community guidelines that prohibit sharing explicit content, enforcement is often inconsistent, and the process for removing such content can be slow. Hence a proper efficient framework coupled with effective redressal in the review process of concerned social media should be implemented.

4. Protection of Youth from XR (Extended Reality) Online Gaming Platforms:

The future of Extended Reality (XR) and gaming is a topic of significant interest, with experts predicting far-reaching impacts on society, entertainment, education, and various industries. By 2040, the metaverse—a shared digital environment—is expected to transform human interaction through immersive experiences that blend physical and digital realities. XR technologies, including virtual reality (VR) and augmented reality (AR), will play a key role, offering spaces for socializing, education, and more. The advent of online gaming has been impacting youth since 2017, when the "Blue Whale Challenge" emerged. A 14-year-old student from Andheri in Mumbai was the first victim of the game to be reported in India. The Blue Whale Challenge is an online game that originated in Russia, notorious for its dark and dangerous nature. It involves players being assigned a series of tasks or dares by a "curator" over 50 days. The initial tasks are relatively simple, such as "wake up in the middle of the night" or "watch a scary movie." However, the challenges progressively become more dangerous, with instructions like "stand on the edge of a tall building" or "carve a whale into your arm." The final challenge tragically compels the player to take their own life. Cybercriminals can use VR environments to identity theft, phishing, or fraud by creating deceptive virtual spaces. XR can also be misused for virtual harassment, bullying, or stalking within immersive platforms. As XR evolves, so do its protection and security vulnerabilities, making it a potential target for hackers and other malicious

actors. The Ministry of Home Affairs (MHA) has issued a warning about frauds related to gaming apps, urging users to exercise caution while engaging in online gaming. The Indian Cyber-Crime Coordination Centre (I4C), part of the MHA's Cyber Wing, has advised users to download apps only from trusted sources, verify the legitimacy of game app publishers, and avoid falling for in-app purchases and subscription scams. As of the year of 2022, the Centre had blocked 581 apps, including 174 betting and gambling platforms and 87 loan lending apps, based on recommendations from the MHA. These apps, blocked under Section 69A of the IT Act, 2000, included popular gaming platforms like PUBG and Garena Free Fire. Many of the betting apps collected UPI payments through proxy bank accounts, with the funds being routed through hawala, cryptocurrency, and other illegal means. Recently, Union Home Minister Amit Shah confirmed that over 500 internet-based applications have been blocked on I4C's recommendation.

Through this research we would like to point out that the National Gaming Commission which overlooks into matters of e-gambling should also emphasise on those applications involving XR, VR and AR, and shall prescribe boundaries within which the algorithms can be used to develop such games. This will ensure that the apps are not violent in nature thereby protecting mental and psychological health of users. The developers must focus on utilising these notable technologies in the field of criminological research, medical training for medical practitioners, surgical simulations and to foster mental health treatment in order to reduce their dependence on unethical human experimentation.

CONCLUSION

Cyberspace has been developing at a rapid pace in the digital era however it falls short on certain aspects such as cyber bullying, online gender-based harassment, sextortion, revenge porn, misuse of deepfake and XR (Extended Reality) which tends to pose a serious problem in the society. This research emphasizes the urgent need to close the gender gap in technology access, advocating for an inclusive digital economy that empowers marginalized groups, especially women. We propose a framework to track social media networks related to non-consensual pornography, improve enforcement of content guidelines, and expedite harmful content removal. Additionally, we call for stringent regulations to ensure unbiased algorithms and secure data encryption in deepfake technology, alongside enhanced detection tools to identify malicious users. We also urge the National Gaming Commission to oversee XR, VR, and AR applications to prevent violent content and protect mental health. These recommendations aim to foster a safer and more equitable digital landscape.

*****

PROSPECTS OF ARTIFICIAL INTELLIGENCE IN TACKLING CYBER CRIMES

***Abhishek Varshney*[15]**

ABSTRACT

As we are living in an interconnected online world, most of our everyday communications and commercial activities now take place via the Internet. Since cyber infrastructure is highly vulnerable to attacks, the threats in cyber space move at the speed of light. With the speed of cyber activity and high volume of data used, the protection of cyber space cannot be handled by any physical device or by human intervention alone. It needs considerable automation to detect threats and to make intelligent real-time decisions. It is difficult to develop software with conventional algorithms to effectively protect against the dynamically evolving attacks. It can be tackled by applying bio inspired computing methods of artificial intelligence to the software. The purpose of this study is to explore the possibilities of artificial intelligence in addressing the cybercrime issues.

Keywords: Artificial Intelligence, Artificial Neural Network, Artificial Immune System, Intelligent Agents, Genetic Algorithm, Fuzzy, Cyber Crime, Intrusion Detection and Prevention Systems.

INTRODUCTION

As we are living in an interconnected online world, most of our everyday communications and commercial activities now take place via the Internet. Growing trends of internet computing raises the questions about the cyberspace‟s information security. Cyberspace is vulnerable to threats and intrusion. Threats in cyberspace move at the speed of light targeting citizens, businesses and governments. It is obvious that defense against intelligent cyber weapons can be achieved only by intelligent software. Due to the high speed of cyber activity and large volume of data used, defense against threats of cyber space cannot be handled by any physical device or by human intervention alone. It needs considerable automation to detect threats and to make intelligent real-time decisions. It is difficult to develop software with conventional algorithms to effectively protect against the dynamically evolving attacks. This is why we need innovative approaches such as applying methods of Artificial Intelligence (AI) that provide flexibility and learning capability to software which will assist humans in fighting cybercrimes. [1]

CYBER CRIMES

With the growth of the Internet, cyber crimes are also growing. Internet crime takes many faces and it is committed in diverse fashion. Cybercrime means that the illegal activities are committed through the use of computers and the internet. The evolution of the internet and its diversity in the world are the sources of cybercrimes. Cybercrime can basically divide into two major categories. One in those takes the network as criminal object such as intrusion, destructing the network system etc. The others are those using the network to commit crime such as fraud [2].

Although “cybercrime” has become a common phrase today, it is difficult to define it precisely. Somaiya et.al. (2014) defines “Cybercrime is a term used widely to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity”[3]. Halder et al

[15] Student at IFTM University, Moradabad, India.

(2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones [4]. According to Kandpal et al (2013)" Cybercrime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cybercrimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc." [5].

The statistics that have been obtained and reported about demonstrate the seriousness of Internet crimes in the world. "Phishing" emails alone produce one billion dollars for their perpetrators. In a FBI survey in early 2004, 90 percent of the 500 companies surveyed reported a security breach and 80 percent of those suffered a financial loss. A national statistic in 2003 stated that four billion dollars in credit card fraud are lost each year. Only two percent of credit card transactions take place over the Internet but fifty percent of the four billion, mentioned before, are from the transaction online. All these finding are just an illustration of the misuse of the Internet and a reason why Internet crime has to be slowed down [6].

ARTIFICIAL INTELLIGENCE

AI (also called machine intelligence in the beginning) emerged as a research discipline at the Summer Research Project of Dartmouth College in July 1956. John McCarthy, who coined the term defines it as "the science and engineering of making intelligent machines" [7]. Universally accepted definition of artificial intelligence is that "Artificial Intelligence is the study of how to make computers do things which, at the moment people do better". The central problems (or goals) of AI research include reasoning, knowledge, planning, learning, natural language processing (communication), perception and the ability to move and manipulate objects. An AI system must be capable of doing three things.

i. Store knowledge

ii. Apply the stored knowledge to solve problems

iii. Acquire new knowledge through experience

AI has three key components –Representation, Reasoning, and Learning [8]. The general problem of simulating intelligence has been simplified to specific sub-problems which have certain characteristics or capabilities that an intelligent system should exhibit.

The following characteristics have received the most attention [9, 10, 11]:

a) Deduction, reasoning, problem solving

b) Knowledge representation

c) Planning

d) Machine learning

e) Natural Language Processing

f) Motion and Manipulation

g) Perception

h) Social Intelligence

i) Creativity

j) General Intelligence

Typical AI methods mainly focus on individual human behavior, knowledge representation, inference procedures. On the other hand, Distributed Artificial Intelligence (DAI) mainly focuses on social behavior. DAI systems can be defined as cooperative systems where a set of agents act together to solve a given problem. These agents are often heterogeneous. According to Jacques Ferber (1999), "An agent can be a physical or virtual entity that can act, perceive its environment (in a partial way) and communicate with others, is autonomous and has skills to achieve its goals and tendencies."[12]. Agents are distinct entities with standard boundaries and interfaces designed for problem solving. Whereas Multi-Agent system is a network of agents which are loosely coupled working as a single entity like society for problem solving that an individual agent cannot solve.

The main applications of multi-agent systems are [12]

- Problem Solving
- Multi-Agent Simulation
- Construction of Synthetic Worlds
- Collective Robotics
- Kenetic Program Design

Computational Intelligence (CI) is a branch of Artificial Intelligence which is mainly focused on heuristic algorithms such as fuzzy systems, neural networks and evolutionary computation. The term „Soft Computing" is mutually interchangeable with Computational Intelligence. More recently, emerging areas such as artificial immune systems, swarm intelligence, chaotic systems, etc. have been added to the range of Computational Intelligence techniques [13]. The nature - inspired techniques such as neural networks, fuzzy logic, evolutionary computation, swarm intelligence, machine learning, and artificial immune system provide flexible decision making mechanism for problems like cyber security issues.

Genetic algorithms are another example of AI technique. They provide robust, adaptive and optimal solutions even for complex computing problems. They can be used for generating rules for classification security attacks and making specific rules for different security attack in intrusion detection systems (IDS) [14,15].

INTRUSION DETECTION AND PREVENTION SYSTEM

Intrusion Detection System (IDS) can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. The firewall defend an organization from malicious attacks from the Internet and the IDS if someone tries to break in through the firewall or manages to break in the firewall security then tries to have access on any system in the trusted side. It alerts the system administrator in case there is a breach in security. An IDS is like a smoke detector, that raise an alarm if specific things occur.

An Intrusion Detection System (IDS) is a device or software that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS can be Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS) [16].

IDS performs a variety of functions [17]:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trials and highlighting user violation of policy or normal activity
- Installing and operating traps to record information about intruders
- Correcting system configuration errors

An **intrusion detection and prevention system (IDPS)** is a software or hardware device placed inside the network, which can detect possible intrusions and also attempt to prevent them [1]

Artificial Neural Networks (ANNs) can enhance the performance of Intrusion Detection Systems (IDS) when compared with traditional methods [17]. Artificial neural networks are a stepping stone in the search for artificial intelligence. ANNs is an information processing system which is inspired by biological nervous system. ANN has tools through which we can develop AI [8].

APPLICATIONS OF AI TECHNIQUES IN DEFENDING CYBER CRIMES

Available academic resources show that AI techniques have numerous applications in cybercrime detection and prevention. For instance, in using neural networks it is possible to develop highly efficient intrusion detection and prevention system. Proposal for using artificial neural networks in the detection of Denial of Service (DoS) attack, computer worm, spam, zombie, and in malware classification and forensic investigation also exists [18]. New generation antivirus systems are using AI techniques such as Data mining, neural networks, and heuristics methods to improve their efficiency [19]. Distributed wireless Intrusion Detection System (IDS) sometimes uses intelligent agents combined with mobile agents [20]. IDS based on mobile agents provide security for the network using mobile agent mechanisms to add mobility features for monitoring suspicious cyber activity [21].

1. Application of Artificial neural networks against cyber crimes

Artificial Neural Network is a massively parallel distributed processor made up of simple processing units, which has a natural capability for storing experimental knowledge and making it available for use [8]. Chen (2008) depicted NeuroNet – a neural network system that is proficient in monitoring the traffic, spot the traffic anomalies, and it triggers countermeasures for it. The experiment results in NS-2 showed that NeuroNet is effective against one type of hidden attack called low-rate TCP-targeted distributed DoS attacks, which is also known as shrew attacks [22] .

Iftikhar et al (2009) designed a system based on ANN to detect probing attacks. It adopted a supervised neural network phenomenon to inspect the feasibility of an approach to probing attacks that are the basis of others attacks in computer network systems. The developed system is applied to different probing attacks and while comparing its performance to other neural networks‟ approaches and the results indicate approach based on Multiple Layered Perceptron (MLP) architecture is more precise and accurate and it shows optimum results as compared to other methods [23]. Linda et.al (2009) presented a novel IDS-NNM – Intrusion Detection System using Neural Network based Modelling which uses a specific combination of two neural network learning algorithms namely Error-Back Propagation and Levenberg -Marquardt for behaviour modelling. Experimental results showing IDS-NNM algorithm is capable of capturing all intrusion attempts presented in the network communication without generating any false alerts [24]. Barika (2009) suggests Artificial Neural Network architecture for decision making within intrusion detection systems with the goal of increased efficiency [25]. Iftikhar et al (2010) presents an evaluation of different neural network systems namely Self-Organizing Map (SOM), Adaptive Resonance Theory (ART), Online Back Propagation (OBPROP), Resilient Back Propagation (RPROP) and Support Vector Machine (SVM) towards intrusion detection mechanisms using the Multi-Criteria Decision Making (MCDM) technique. The results show that in terms of performance, supervised NNs are better, while regarding training overhead and aptitude towards handling varied and coordinated intrusion unsupervised NNs are better. From this the conclusion is that Hybrid approach of NNs is the optimal solution in the area of intrusion detection [26].

Brij (2011) ANN is employed to estimate number of zombies involved in a flooding DDoS attack which is helpful to suppress the effect of attack [27]. Wu (2009) presented a hybrid method for spam filtering which uses rule-based processing and back-propagation neural networks. Since the spamming behaviours may frequently change, this method has proven to be much more robust compared to other spam detection approaches that consider keywords [28]. Kufandirimbwa and Gotora (2012) presented a technique to spam filtering using Artificial Neural Networks, and the perception learning method which produces favourable detection rates due to the incorporation of a continuous learning feature as compared to other spam detection methods based on content and other characteristics of the message [29].

Venkatesh et al (2012) presented a Multi-Layer Feed Forward Neural Network training model using Bold Driver Back-propagation learning algorithm for HTTP Botnet

detection which has a good identification accuracy with less false positives [30]. Devikrishna et al (2013) presented A Multi-Layer Perception (MLP) for intrusion detection and used Knowledge discovery in Database (KDD) for classification of attacks [31]. Zhai (2014) proposed a multi-agent distributed IDS (DIDS) model based on BP neural network for intrusion detection with the advantages of reducing the amount mobile process of data, load balancing, detecting analysis neatly, better error-tolerating, and detecting distributed intrusion effectively [32].

2. Application of Intelligent agents against cyber crimes

Intelligent agents are autonomous computer-generated forces with the capability to communicate with each other to share data and they can cooperate with each other in order to plan and implement appropriate responses in case of unexpected events. The intelligent agents‟ characteristics like mobility, adaptability in the environments they are deployed in, and their collaborative nature, makes them suitable for combating cyber attacks. Rowe (2003) developed a tool to systematically counter plan the ways to prevent particular cyber attack plans using multi-agent planning and some novel inference methods [33]. Helano (2006) introduced a system implemented in Prolog which is a synthesis based on a multi-agent systems (MAS) approach with a practical case used to fight cyber intrusions and with the ability to verify the properties of cybercrimes [34]. Mueen Uddin et.al (2010) proposed a new model called Dynamic Multi-Layer Signature based IDS using Mobile Agents, which can detect forthcoming threats with very high success rate by dynamically and automatically creating and using small and efficient multiple databases, with a mechanism to update these small signature databases at regular intervals using Mobile Agents [35] . Mayank et al (2011) simulated dynamic mobile agent model using Colored Petri Nets (CPNs) which enables the owner of the agent to detect the malicious host. The simulation result clearly proves that owner can detect the malicious hosts and thus prevent Denial of service attack to occur in real world [36]. Akyazi et al (2012) proposed a distributed intrusion detection system to detect Distributed Denial of Service attacks in a special dataset. This method is tested in a simulated-real time environment, in which the mobile agents are synchronized with the timestamp given in the dataset [37].

Onashoga et al (2013) proposed a Multi agent-based architecture for Intrusion Detection System (IDS) to overcome the shortcoming of current Mobile Agent-based Intrusion Detection System, with three major phases namely: Data gathering, Detection and the Response phase [38]. M. Rajesh Kanna et al (2013) designed a wireless distributed Wireless Intrusion Detection System (WIDS) based on Intelligent agents which consist four major components: Intrusion detection module, Alert, Mobile agent platform, Test suit [20].

3. Application of artificial immune system against cyber crimes

Artificial Immune Systems (AIS) are a class of computationally intelligent systems which imitate the biological immune systems. Since the artificial immune system has techniques to solve complex computations, AIS plays an important role in the cyber security research. Zhang et al (2011) proposed a hierarchical Distributed Intrusion Detection SGDIDS namely SGDIDS System that is applicable to identification of malicious network traffic and improving system security for improving cyber security

of the Smart Grid with an intelligent module. This system uses AIS to detect and classify malicious data and possible cyber attacks [39]. Amit Kumar et al (2012) proposed a new general HTTP Botnet detection framework for real time network using Artificial Immune System (AIS) with no need for prior knowledge of Botnets [40]. Ismaila (2012) proposed a spam detection model based on negative selection algorithm that generates a new self (system) that randomly creates antibody against spam, by distinguishing self from non-self. The experimental result guarantees that the proposed model is able to establish a better true positive on an unknown spam [41]. Smera et al (2014) studied and compared two efficient spam filters namely Bayesian filters and Artificial Immunity filters and suggested Bayesian classifier has as an effective method to construct anti-spam filters [42]. Ibor et al (2015) proposed a highly efficient hybrid technique which is achieved using the combined features of three algorithms namely J48, Boyer Moore and K-NN for Malicious Network Traffic based on Active Response [43].

4. Application of genetic algorithm and fuzzy against cyber crimes

Liu et al (2010) to detect computer virus, the clustering method combining genetic algorithm and ant colony algorithm is adopted. From experimental results, it is clear that this method exhibits strong adaptability, shows better intelligence, and higher degree of automation in detecting virus [44].

Linda et al (2011) proposed a novel fuzzy based learning algorithm for anomaly based network security cyber sensor together with its hardware implementation. The anomaly detection algorithm was specifically designed to allow for both fast learning and fast classification of attacks [45]. Hoque et al (2012) presented an Intrusion Detection System (IDS), by applying Genetic Algorithm (GA) to efficiently detect various types of network intrusions using the standard KDD99 benchmark dataset [46]. Ojugo et al (2012) presented a genetic algorithm based approach with its driver implementation. It employs a set of classification rule derived from network audit data [47]. Jitendra (2013) presented a genetic algorithm to detect email spam and the proposed idea is tested on 2248 mails and the overall efficiency is nearly 82% [48]. Jongsuebsuk et al (2013) depicted a network IDS based on a fuzzy genetic algorithm. Fuzzy rules are used to classify network attack data, whereas genetic algorithm optimizes the solution. The evaluation results showed that the proposed IDS can detect network attacks in real-time and within 2-3 seconds upon the arrival of data with the detection rate of over 97.5% [49]. Roshna et al (2013) presented a technique named as botnet detection using Adaptive Neuro Fuzzy Inference System (ANFIS) based on Anfis algorithm [50].

AI flexible features for IDPSs AI techniques have numerous traits that make it suitable for the construction of the intrusion detection and prevention system (see Table 1)

Table 1: AI features for IDPS Technology	**Features**
Artificial Neural Networks	i. Learning by example. ii. Resilience to noise and incomplete data. iii. Intuitiveness since it mimics biological neuron.

Intelligent Agents	i. Mobility. ii. Adaptability. iii. Collaboration.
Artificial Immune Systems	i. Self-adaptability. ii. Self-organizing. iii. Dynamic nature.
Genetic Algorithms and Fuzzy	i. Optimization. ii. Robustness. iii. Flexible.

LIMITATIONS OF EXISTING ANOMALY DETECTION AND PREVENTION SYSTEM

Today IDPS have become extremely valuable in enhancing the security of the networks and end hosts; they however have numerous key drawbacks [51].

They are:

- Encryption: Once the data packets are encrypted, the existing detection mechanisms may become completely futile in identifying the intrusions.
- Evasion of signatures: polymorphic worms which can automatically change their propagation characteristics thereby changing their signatures. Such worms also constitute a critical threat to the current detection system.
- False Positives: A false positive is an incident when a IDS falsely raises a security threat alarm for harmless traffic.
- Legal regulations: intrusion detection systems need to conform to legal regulations
- Attack to IDPS: may be disabled by attackers if they can learn how the system works.

CONCLUSION

As we are living in an online world, most of our everyday communications and commercial activities now take place via the Internet. However, it also caused issues that are difficult to manage such as the emergence of cyber crimes. Available academic resources show that AI techniques already have numerous applications in combating cyber crimes. This paper has briefly presented possibilities of AI techniques so far in cyber field for combating cyber crimes and their current limitations.

*****

REFERENCES

[1] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, ”Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015

[2] Manveer Kaur, Sheveta Vashisht, Kumar Saurabhi, “Adaptive Algorithm for Cyber Crime Detection”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012

[3] Jheel Somaiya, Dhaval Sanghavi, Chetashri Bhadane, ”A Survey: Web based Cyber Crimes and Prevention Techniques”, International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014

[4] Halder, D. Jaishankar, K, ”Cyber crime and the Victimization of Women: Laws, Rights, and Regulations”. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

[5] Vineet Kandpal and R. K. Singh, ”Latest Face of Cybercrime and Its Prevention In India”, International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013

[6] Advocate, Vivek Tripathi,” Internet Crime”, www.cyberlawsindia.net, Available: http://www.cyberlawsindia.net/internet-crime.html

[7] V. Rajaraman, ”JohnMcCarthy – Father of Artificial Intelligence”, in General Article Resonance, March 2014

[8] T N Shankar, Neural Networks, LAXMI Publications Pvt.Ltd, 2008

[9] J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003

[10] G. Luger, W. Stubblefield, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Addison Wesley, 2004.

[11]Wikipedia, “Artificial Intelligence”, en.wikipedia.org, Available: http://en.wikipedia.org/wiki/Artificial_intelligence

[12] Jacques Ferber, Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman, 1999

[13]UKCI, “Workshop on Computational Intelligence”, ukci.cs.manchester.ac.uk, Avaliable: http://ukci.cs.manchester.ac.uk/intro.html

[14] N. A. Alrajeh and J. Lloret,” Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, Vol.2013, Article ID 351047.

[15] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, A. Patel, “An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique,” Engineering Applications of Artificial Intelligence, Vo. 26, pp. 2105–2127.

[16]Wikipedia, “Intrusion detection system”, en.wikipedia.org, Available: http://en.wikipedia.org/wiki/Intrusion_detection_system

[17]Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, ”A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering”, Elsevier Ltd 2010

[18] E. Tyugu, ”Artificial intelligence in cyber defense”, In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11,2011.

[19] X. B. Wang, G. Y. Yang, Y. C. Li and D. Liu, ”Review on the application of Artificial Intelligence in Antivirus Detection System”, In Proceedings of the IEEE Congress on Cybernetics and Intelligent Systems, pp. 506- 509,2008

[20]M Rajesh Kanna, D. Hemapriya and C. Divya,” Intelligent Agents For Intrusion Detection System (IAIDS)”, International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 3, January 2013. [21]N. Jaisankar, R. Saravanan, K.Durai Swamy, “Intelligent Intrusion Detection System Framework Using Mobile Agents”, International Journal of Network Security & Its Applications (IJNSA), Vol 1, July 2009

[21]Yu Chen, ”NeuroNet: Towards an Intelligent Internet Infrastructure”, In Proceedings of the 5th IEEE Congress on Consumer Communications and Networking Conference (CCNC), pp. 543 547,2008

[22] Iftikhar Ahmad, Azween B Abdullah, and Abdullah S Alghamdi, ”Application of Artificial Neural Network in Detection of Probing Attacks”, In Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA), 2009

[23]Ondrej Linda, Todd Vollmer and Milos Manic, ”Neural Network Based Intrusion Detection System for Critical Infrastructures”, In Proceedings of the International Joint Congress on Neural Networks, 2009

[24] F. A. Barika, K. Hadjar, and N. El Kadhi, ”Artificial Neural Network for Mobile IDS Solution”, Security and Management, pp. 271–277.

[25] IftikharAhmad, AzeenAbdullah, and Abdullah Alghamdi, ”Towards the selection of best neural network system for intrusion detection”.

[26]Brij Bhooshan Gupta, Ramesh Chand Joshi, and Manoj Misra, ”ANN Based Scheme to Predict Number of Zombies in a DDoS Attack”, International Journal of Network Security, Vol.14, PP. 61–70, Mar 2012

[27] C. H. Wu, “Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks”, Expert Systems with Applications, Vol. 36, pp. 4321–4330.

[28]Owen Kufandirimbwa and Richard Gotora, ”Spam Detection Using Artificial Neural Networks (Perception Learning Rule), Online Journal of Physical and Environmental Science Research, ISSN 2315-5027; Volume 1, pp. 22-29; June 2012

[29]G Kirubavathi Venkatesh, and Anitha Nadarajan, ”HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network”, International Federation for Information Processing 2012

[30]Devikrishna K S and Ramakrishna B B, ”An Artificial Neural Network based Intrusion Detection System” and Classification of Attacks”, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 , Vol. 3, pp. 1959-1964, Jul-Aug 2013

[31]ZhaiShuang-can, Hu Chen-jun and Zhang Wei-ming, ”Multi-Agent Distributed Intrusion Detection System Model Based on BP Neural Network”, International Journal of Security and Its Applications Vol.8, pp.183- 192, 2014.

[32] N. C. Rowe, “Counterplanning Deceptions To Foil Cyber-Attack Plans”, In Proceedings of the 2003

[33]IEEE Workshop on Information Assurance, pp. 203 210

[34] José Helan and Matos Nogueira, ”Mobile Intelligent Agents to Fight Cyber Intrusions”, International Journal of Forensic Computer Science , IJoFCS, pp 28-32,2006

[35]Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman, ”Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents”, International Journal of Network Security & Its Applications (IJNSA), Vol.2, October 2010

[36]Mayank Aggarwal, Nupur and Pallavi Murgai, ”Simulation of Dynamic Mobile Agent Model to Prevent Denial of Service Attack using CPNS”, International Journal of Computer Applications Volume 20, April 2011

[37]Ugur Akyazi , and A. Sima Uyar, “Distributed Detection of DDOS Attacks During the Intermediate Phase Through Mobile Agents”, Computing and Informatics, Vol. 31, 759–778, 2012

[38]Onashoga, S. Adebukola, Ajayi, O. Bamidele and Akinwale, A. Taofik, ”A Simulated Multiagent-Based Architecture for Intrusion Detection System”, International Journal of Advanced Research in Artificial Intelligence (IJARAI), Vol. 2, 2013

[39] Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, “Artificial Immune System based Intrusion Detection in A Distributed Hierarchical Network Architecture of Smart Grid”, IEEE Power and Energy Society General Meeting, pp. 1 – 8, 2011

[40]Amit Kumar Tyagi and Sadique Nayeem, “Detecting HTTP Botnet using Artificial Immune System (AIS)”, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 , Volume 2, May 2012

[41] Ismaila Idris,” Model and Algorithm in Artificial Immune System for Spam Detection”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, January 2012

[42]Smera Rockey and Rekha Sunny T , “A Hybrid Spam Filtering Technique Using Bayesian Spam Filters and Artificial Immunity Spam Filters”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181,Vol. 3 , May – 2014

[43]Ayei E. Ibor and Gregory Epiphaniou, ”A Hybrid Mitigation Technique for Malicious Network Traffic based on Active Response”, International Journal of Security and Its Applications Vol. 9, pp. 63-80, 2015

[44]Liu Guozhu and Shang Yanjun, ”Unknown Virus Detection Method Amalgamation Genetic Algorithm into Ant Colony Algorithm”, Journal of Computers, Vol. 5, June 2010

[45]Ondrej Linda, Milos Manic, Todd Vollmer and Jason Wright”, Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor “, In IEEE Symposium on Computational Intelligence in Cyber Security, 2011

[46]Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, “An Implementation of Intrusion Detection System Using Fenetic Algorithm”, International Journal of Network Security & Its Applications (IJNSA), Vol.4, March 2012

[47]A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs) and F.O. Aghware, “Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)”,Journal of Emerging Trends in Computing and Information, ISSN 2079-8407, Vol. 3, Aug 2012

[48] Jitendra Nath Shrivastava and Maringanti Hima Bindu, ”E-mail Classification Using Genetic Algorithm with Heuristic Fitness Function”, International Journal of Computer Trends and Technology (IJCTT) – volume 4 August 2013

[49] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, "Real-time intrusion detection with fuzzy genetic algorithm," In Proceedings of the 10th International Congress on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 1-6, 2013

[50]Roshna R.S and Vinodh Ewards, ”Botnet Detection Using Adaptive Neuro Fuzzy Inference System”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, pp. 1440-1445, March -April 2013

*****

BEHIND THE SCREEN: UNDERSTANDING AND COUNTERING CYBER-TERRORISM IN MODERN WARFARE

Nivedita Mahesh[16]

ABSTRACT

In today's digital age, the battlefield has expanded beyond borders and physical space, with Cyber-Terrorism becoming one of the most used weapons in modern warfare. Cyber Attacks such as the August 2022 DDoS attack on the Finnish Parliament and Russia's continued use of cyber attacks on Ukranian infrastructure despite the existence of 18 conventions dealing with these issues have highlighted the need for active international cooperation to combat this new form of warfare. Defined as deliberate attacks by recognised terrorist organisations against computer systems, Cyber-Terrorism is designed to incite panic and destruction. In these circumstances, Leon Panetta's words "The potential for the next Pearl Harbor could very well be a cyber-attack", might as well be a real concern. The devastating consequences of cyber attacks were made clear in a 2023 study from the University of Minnesota, which revealed that between 42-67 US Medicare patients died due to ransomware incidents between 2016 to 2021. Thus, the destructive potential of Cyber-Terrorism ranges from blackouts to systematic collapse. The threat to civilian life and infrastructure is immense, as these attacks may eventually pave the way for larger terrorist operations. This paper is divided into key sections addressing the following: an analysis of real instances of the use of Cyber-Terrorism in warfare, understanding the motivations behind these attacks and their impact, and considering recent developments in AI that could help detect and neutralise cyber threats. The research methodology employed in this paper is qualitative, primarily relying on secondary data, drawing from reports, and official records from real incidents. Ultimately, this paper discusses measures, not just by preparing states in this battle against computers, but also against the individuals hiding behind the screen, destroying countless lives.

Keywords: Cyber-Terrorism, Cyber-Espionage, Modern Warfare, AI in Cyber Security.

INTRODUCTION

"Tomorrow's Terrorist may be able to do more damage with a keyboard than with a bomb"

- National Research Council

The concept of Cyber-Terrorism is not one that evolved overnight, rather it has been perfectioned over decades as the internet evolved into a crucial part of human life, almost as important as one's limb. As the information age began between the late 1980s to early 90s, there came the realisation that the technology that we depend on today could be maliciously used against us. This potential was first apparent when in 1988, a University student accidentally unleashed the Morris Worm infecting 6,000 systems. This fear was later intensified when in 1997, an NSA experiment revealed that hackers could access critical Pentagon systems, tamper with evidence, access classified information and shut down networks, all without stepping inside the building with the most basic phishing techniques.

By the early 2000s, Cyber-Terrorism became a weapon for ideological conflict as terror inflictors realised its potential. One such instance originated in Iraq where a network of over 100 websites known as "Iraq Net" was supposedly set up to launch DoS (Denial of Service) attacks on U.S corporations,

[16] Student at Ramaiah University of Applied Sciences, Bengaluru, India.

being able to render useless, the most important computer systems across corporations. Based on this context, Yonah Alexander, a terrorism researcher remarked that "Sadam Hussein would not hesitate to use the cyber tool" Similarly, Jihadist groups have also explored the potential of an "Electronic Jihad" undermining Western infrastructure. The Handbook by Mohammad Bin Ahmad As-Sālim, "39 Ways to Serve and Participate in Jihad" is one such call for cyberattacks that may destroy American websites and other such entities that may seem hostile to the Jihadist cause. Non-state actors like the Islamic State's "Cyber Caliphate Army" signal a broader use of cyber warfare for military, political or ideological goals.

From its conception, Cyberterrorism aimed to not only dismantle critical systems that humans rely heavily on but also instil panic across society. The fact that this type of terrorism is so remote that a hacker working in the Northern Hemisphere may upend entire societies in the Southern Hemisphere is certainly nerve-wracking. It became evident that without firing a single missile, a whole war could be declared through advanced hacking tactics. The fear of the unseen disrupting lives deeply impacts the public psyche. In 2016, India ranked among the top 5 countries that are most vulnerable to cyberattacks. Hacking groups like Transparent Tribe based in Pakistan which are notorious for targeting Indian Defence sectors, pose an increasing threat in South Asia in terms of Cyber espionage and disruption. Such attacks are reflective of the increasing scope and sophistication of Cyber- Terrorism, that too, so close to home.

The 21st century saw a significant evolution like cyberattacks, for instance, the proliferation of suspicious apps and targeted cyberattacks during the COVID-19 pandemic in 2020 and 2021 demonstrated how cybercriminals can take advantage of global emergencies and crises. According to Trend Micro, in the first quarter of 2021 alone, over 164 malicious apps were found, taking advantage of our reliance on digital connectivity during lockdown. Thus, the convergence of technology and terrorism has now become a formidable tool for both state and non-state actors to use as part of Cyber Warfare or even to further an ideological or political cause, which shall be further examined in the upcoming sections.

REAL-TIME CONSEQUENCES OF CYBER-TERRORISM

India with the second-largest online market in the world has, as previously mentioned, been especially susceptible to Cyber-Terrorism. Incidents such as the URI attack, Pulwama and the 26/11 Mumbai attacks stand as glaring examples of how technology in the wrong hands can have devastating effects. Especially during the 26/11 attacks, the terrorists used Google Earth, social media and mobile networks, as do common people. This is very similar to how the 9/11 terrorists operated, using hacking mechanisms to procure fake IDs, steal Social Security numbers, etc. Such attacks not only result in loss of lives but also instil fear about future attacks and undermine cybersecurity frameworks. Those who feared future attacks in 26/11 were probably right in doing so, as evidenced by the report from CERT-In revealing that in 2022 alone there were over 1.39 million cybersecurity attacks. When such are the numbers, ordinary civilians such as ourselves cannot even feel secure in our own homes, working on our systems. How are we to feel safe when Pakistani Cyber Criminals deface nearly 60 Indian websites every day? This fear was especially highlighted in a study by the Pew Internet and American Project

which found in 2003 that nearly half the Americans surveyed were concerned about Cyber- Terrorist attacks. The study revealed that while 38% of the participants were somewhat worried about such attacks, 11% had some serious concerns.

In July 2022, Chinese Advanced Persistent Threat actors launched an attack on Belgium's government and military, to gather intelligence and steal trade secrets. What is surprising to note is that this attack was sponsored by the Chinese government itself, demonstrating how Cyber-Terrorism is also used in State-sponsored espionage activities. On a similar line was the 2014 Sony cyberattack, which was linked to North Korea. The attack was deemed to be in response to the controversial Sony film "The Interview", satirising North Korean leader Kim Jong Un. Threats of physical terrorist attacks on theatres playing the movie were also made through this cyberattack.

Another such instance is the use of cyber-warfare tactics such as the 2010 Stuxnet worm, allegedly developed by the U.S. in conjunction with Israel which severely disabled Iran's nuclear infrastructure. Such attacks include China's breach of the U.S. Office of Personnel Management in 2015 and Russia's interference in the 2015 U.S. presidential election. These examples prove the impact of cyberattacks on the day-to-day functioning of a government or the capability to undermine a nation's democratic process.

Russia and Ukraine

Throughout the conflict, cyberattacks have been used alongside conventional warfare to disrupt civilian life and infrastructure using techniques such as wiper malware that permanently alters data and the attack on the Viasat satellite network that cut off the internet across parts of Ukraine and Europe, affecting wind turbines in Germany and around 9,000 subscribers in France. A malware attack also breached the process of allowing refugees into Romania. Such attacks have mainly targeted water, power and communication infrastructure, leaving many Ukrainians devoid of essential resources. This was accompanied by infiltration of media with false information. At one point the mass was falsely led to believe that President Zelensky was incapacitated, causing chaos. As mentioned previously, even some of Europe has been victim to the effects of these cyberattacks. Unlike physical war, cyber warfare tends to cause direct effects in areas outside the conflict zones as well.

The case of Hamas and Israel

While the world has been focused on missiles and rockets, a parallel war is taking space in cyberspace. Hamas has been known for employing cyberattacks ranging from phishing schemes to DoS attacks on news outlets, banks and hospitals. For instance, on the dreadful day of October 7th, 2023, Hamas hackers infiltrated the 'RedAlert' app used to warn civilians about impending strikes and threats, making the attack completely unprecedented. Meanwhile, Israel has used internet blackouts in Gaza as part of its attempt to cripple communication channels among militants, garnering international criticism over this response. These instances just to name a few of the many that may be involved in the Israel-Hamas war demonstrate a poignant example of how Cyber-Terrorism is used in modern warfare, in hampering alerts sent to civilians thereby causing a breakdown of digital as well as physical infrastructure.

One may notice that in all these instances, the one common impact has been on civilian lives. Any act ranging from the hacking of Jerusalem Post's website to the disabling of Indian Defence Systems by cyber espionage sends a message to the civilians: "When it comes to cyberattacks, even your country cannot protect you". In some unfortunate instances, it is nations themselves that are engaging in attacks of such nature. Nevertheless, the individuals operating behind these screens know one thing for sure, that people fear the unknown or the invisible and that is exactly what gives these individuals the confidence to thrive on our anxiety.

CYBER-TERRORISM OR AFFORDABLE TERRORISM?

The COVID-19 pandemic as discussed, has been a vulnerable period for the rest of the world and a thriving period for cyberattacks. With most of the world shifting towards digital platforms for school or work, the time to carry out cyberattacks could not have been better, it was as if all the targets had gathered in one place, like sheep in a pen awaiting their slaughter. A Statista survey of IT security professionals worldwide revealed that between the first quarter of 2020 and July of 2022, cyberattacks such as data leakage saw a 55% increase and other attacks like phishing emails, ransomware and account takeovers increased by 51%.

Unlike conventional terrorism which requires financial aid, considerate planning and other resources, Cyber- Terrorism can be carried out at a fraction of their costs, thus emerging as a form of "Affordable Terrorism", making it easier for infiltrators to cause a whole lot more damage than incurred by them. Carrying out conventional forms of terrorism can generally cost a lot for the terrorists themselves. For this purpose, ISIS has an estimated war chest of around $2 billion financed by oil smuggling. Likewise, the 9/11 attacks seemed to have cost Al-Qaeda between $400,000 to $500,000 to train and transport the terrorists. Other instances including the 2004 Madrid train bombings and London car bomb attacks cost terrorists between $10,000- $14,000, regardless of whether their missions were a success or a failure. In stark contrast to this, cyberattacks are relatively "affordable" for terrorists. Carrying out a cyber attack is cheaper than committing to cybersecurity itself, this proportion is simply unfair. Armor's Black Market report finds that Personally Identifiable Information is available for less than $200 per record while credit card information can cost as little as $10. Entire accounts containing up to $15,000 can be bought for around $1000. Hacking tutorials can be purchased for around $5 and basic malware can be obtained for $45 as per Top10VPN's Hacking Tools Price Index. While these attacks may be cheap for the perpetrators, they are anything but that for victims. The expenses incurred come not only in the form of money lost but also loss of crucial data, malfunctioning of essential services, damaged reputations and even loss of lives.

Another factor is that while traditional terrorism is localised to one area at a time, Cyber- Terrorism can cause widespread damage. For example, the infamous "ILOVEYOU" virus in 2000, through careful social engineering impacted users across the globe within hours. This proved that cyberattacks may not only be of a large scale but may be immediate as well. Thus, the ability to conduct Cyber- Terrorism remotely furthers its appeal. When you work remotely, leave a lesser impression than you do in person. This may be the logic behind why there is lesser accountability for those operating anonymously behind screens. This gives them a sense of impunity and lessens the likelihood of their capture or death. But

we must make no mistake, hiding behind a screen does not make Cyber- Terrorism any less devastating. The anonymity that those behind the screens hold does not wash the blood on their hands. The keyboard has become today's weapon of terror and it has the potential to reach beyond the other end of the screen.

MEASURES

India, realising the gravity of the threat imposed in cyberspace, has been proactive in taking up measures to strengthen its cybersecurity framework. New encryption and privacy policies are in place. The National Cyber Policy of 2013 laid the base for a national strategy alongside recent initiatives for digital empowerment. However, Section 66F of the Information Technology Act (Amendment), 2008 is currently the only provision in the nation directly addressing Cyber-Terrorism. The evolving nature of cyber threats calls for a stronger framework in this arena. To meet the fast-growing complexities and sophistication of Cyber- Terrorism, India and other nations alike must evolve in tandem with emerging technologies. International cooperation and robust public-private partnership models are needed in the wake of cyberattacks on both states and corporations and even on other entities.

Along with these measures, understanding the motivations behind Cyber- Terrorism may yield an even more robust framework of response. Knowing underlying factors can help us better understand what crucial sectors of society may require more security or what demography of netizens are being targeted, allowing the prioritisation of security in certain areas. There may be a myriad of motivations driving cyberattacks, money, politics and ideology being the heart of such causes. In certain dire situations, the motivation may even be the mere sense of accomplishment that comes with dismantling huge systems. Some treat it as a sport, the bigger the bragger. While Cyber- Terrorism increases anxiety and militancy regardless of the motivations behind it, the context of its operation matters. The identity of the perpetrator or their cause helps explain their attitude towards the cyberattack. For instance, knowing that the LTTE is behind a cyberattack may mean something different to a Sri Lankan or Indian as it may to, say, a Canadian national.

Recent Developments in AI that may help neutralise cyber threats

However, the fight against Cyber- Terrorism is not just a matter of international cooperation or policy, it is also a technological arms movement. As cyber threats are evolving into more sophisticated forms, we must employ the latest innovations and advances in Artificial Intelligence to neutralise these threats. Artificial Intelligence or AI, in particular, can be used in its full capacity to identify these threats before major damage is caused. As per a survey by The Economist Intelligence Unit, 48.9% of security experts and executives consider AI and machine learning as potential tools to combat modern security threats. Machine learning when backed by data science and relevant areas of technological study can prove to be a very useful tool in this war against Cyber- Terrorism. For instance, a global bank used Paladon's AI-based Managed Detection and Response Service to detect advanced attacks, data leakage, ransomware and malware attacks based on data science and machine learning capabilities.

AI can detect new as well as current attacks by analysing consistent patterns and training neural networks to recognise suspicious activities in the initial stage itself. This manner of predictive detection was in use by CompStat, an early form of AI which was also used by the NYPD in "predictive policing".

AI can also detect anomalies or entities out of the ordinary that may signal a polymorphic malware attack. Even before the advent of Cyber- Terrorism, AI-based tools like Armorway used AI to predict terrorist threats to port security in cities like New York and Boston. By using this predictive tool, coupled with an understanding of Cyber-Terrorist motivations, cybersecurity systems can anticipate and timely stop attacks before they may even be executed.

Another subset of AI known as "Deep Learning", can identify patterns through its vast neural networks. It is especially useful in countering malware attacks that rewrite codes to slip past traditional detection methods. By recognising behavioural patterns, even if the code is altered by the attacking entities, Deep Learning models can reduce the time taken for detection. Additionally, Supervised Machine Learning with the help of known datasets of previous incidents, can block emerging threats. This model is used by Extended Detection and Response systems to improve threat identification and mitigation steps.

Certain new developments in AI also allow for what is known as "threat deception". This advanced method allows AI to create artificial environments to trap or mislead cyber attackers, in a manner, borrowing a page from their book. These environments use decoys to interact with the cyber attackers while deterring their attacks at the same time. This type of technology helps cybersecurity frameworks stay ahead of their adversaries.

AI can thus rapidly detect potential threats in real-time, improve accuracy in detecting the said threats, identify vulnerabilities in a system before attackers may exploit them and automatically respond with security measures such as blocking attacks and isolating attacked systems to contain cyberattacks. However, cybersecurity systems must stay ahead of the game as AI is also being increasingly adopted in cyberattacks. While AI may be automated in its tasks, human involvement is essential in assessing threats and making informed decisions towards alleviating them. Fighting Cyber- Terrorism thus requires a multi-layered approach. From framing policies that secure the interests of our cyberspace to using AI against impending cyberattacks, this war on our digital space requires our full efforts to avert dire consequences. All these mechanisms alongside an understanding of what factors motivate such attacks can save the world a lot of loss, both in terms of material assets and human lives.

CONCLUSION

Bruce Schneier once remarked, "Only amateurs attack machines, professionals target people". We are now ironically at a juncture where people are targeted through machines, by other persons hiding behind the safety of a screen. As nations and institutions struggle to brace their defences against unpredictable attacks, it is clear that Cyber- Terrorism has achieved its goal - being a continuing fear among the masses. The anonymity enjoyed by the attackers makes them more dangerous. The scariest is the unknown, something one cannot see, touch or feel but one is aware of. Such is the nature of Cyber-Terrorism. It is time the various nations, institutions and corporations around the world understand that modern warfare is not limited to land, air, or sea; we are now moving towards the realm of cyberspace where the threats can be equally devastating and far-reaching. The fight against Cyber- Terrorism is a race against technology and more importantly, against some of our own kind, willing to stop at nothing.

*****

SAFEGUARDING COPYRIGHT PROTECTION IN AI LEAD REIGN: DEMYSTIFYING THE ENFORCEMENT THROUGH JUDICIAL PRECEDENTS

Meghna Nair[17] and Dr Prabhdeep Kaur Malhotra[18]

ABSTRACT

The rise of Artificial Intelligence ("AI") in literary authorship has raised significant ethical, legal, and intellectual property concerns. Imagine purchasing a book by your favourite author, only to discover later that it was written using AI. While some readers might not mind, others value the authentic expression of the author's own thoughts, not computer-generated content which raises ethical concern in the literary world. Due to advancements in machine learning and generative AI, driven by the vast amounts of data fed into these systems, protected works are in threat of being treated as mere training data for AI models. When the AI companies which may or may not have the legal rights to use such protected works, generate content based on user prompts, the user might unknowingly incorporate someone else's copyrighted material, often without proper citation or acknowledgment. The integration of AI in literary authorship presents significant challenges to existing copyright laws and ethical standards, particularly concerning the unauthorized use of copyrighted material in AI training. It is hypothesized by the author that the liability for copyright infringement primarily lies with the user of the AI-generated work, as they are responsible for the plagiarized content and didn't deploy their own novel thoughts, thereby lacking intellectual footing. Furthermore, since AI is not a natural person and copyright protection is granted only to human authors, literary works created using AI do not qualify for protection under current laws. This paper examines the challenges of AI-generated literary works, focusing on the potential infringement of copyrighted material used in training AI models. It explores the ethics of using protected works without the authors' consent and addresses the issue of liability. The paper also investigates the extent of copyright protection for AI-assisted literary works and the criteria for determining authorship in this context. By analysing these issues, the author aims to contribute to the ongoing discussion on AI, authorship, and intellectual property rights.

Keywords: Intellectual Property, Artificial Intelligence, Literary Authorship, Copyright Infringement, Data Usage Ethics etc.

INTRODUCTION

Humans, as mammals with highly developed brains, have used our intellectual abilities to analyse, discover, and invent a vast array of things—from everyday tools to sending a man to the moon. This remarkable capacity to think, innovate, and problem-solve has positioned humans at the top of the food chain, establishing us as apex predators. However, this dominance and advancement did not happen overnight; it evolved gradually over time, fuelled by the encouragement of creativity and innovation. One of humanity's unique traits is the ability to bring ideas to life through various forms of expression and mediums. Whether through art, literature, or scientific inventions, humans possess the novel ability to create. Naturally, the inventions and creations resulting from this process belong to their creators. However, in earlier times, there was no legal recognition or protection of these intellectual properties. This lack of protection exposed these creations to the risk of being exploited or stolen by others.

[17] LL.M. Student at Amity University Noida, India.
[18] Assistant Professor at Amity University Noida, India.

It is easy to imagine the negative consequences this posed on innovation. Although it is in human nature to think and create, it is also natural for individuals to seek recognition and reward for their efforts. If creators were not granted the right to fully benefit from their creations, many would likely be discouraged from innovating, or they might withhold their creations from public use. This realization became especially prominent during the Enlightenment period, a time of intellectual and cultural awakening. It was during this era that the need to protect the rights of creators and inventors, granting them exclusive control over their intellectual property (IP) begun forming shape. These protections ensured that creators could enjoy the fruits of their labour, which in turn fostered innovation and further allowed the society to benefit from them. This system of protection laid the groundwork for modern intellectual IPR, promoting creativity while ensuring that inventors or authors could thrive in a world that values their work.

WHO IS AN AUTHOR AND WHAT ARE THEIR RIGHTS?

Before delving into the specifics of an author's rights under copyright law, it is essential to first understand who exactly qualifies as an "author". The concept of an "author", especially in the context of Copyright, goes beyond the layman understanding of the term as simply a writer of literary works. The Copyright Act of 1957 defines the term "author" under Section 2(d) of the Act. The definition makes it clear that the legal understanding of author is more nuanced and inclusive, recognizing the author as the creator of various forms of intellectual outputs. In certain cases, such as joint authorship, where multiple individuals contribute to the creation of a work, all contributors may be regarded as co-authors if their contributions are significant and inseparable from the overall creation.

Author's rights under copyright law are bifurcated into Economic and Moral rights. Economic rights allow authors to financially benefit from their work by controlling its reproduction, distribution, performance, and adaptation, as well as earning royalties from their use. These rights can be transferred or licensed to others, enabling commercial exploitation of the work. In contrast, moral rights protect the author's personal connection to their creation. These include the right to attribution, the right to protect the work's integrity, and the right to prevent false attribution. Moral rights ensure that the author's reputation is preserved and that their work is not to be altered in a way that distorts its original intent. While economic rights can be assigned or sold, moral rights are generally non-transferable and remain with the author to safeguard their personal interests. Together, these rights enable authors to maintain control over their work while benefiting from its commercial use.

Can AI be Regarded as an Author?

A key element of the legal definition of an author is that it generally refers to a "natural person", someone capable of independent thoughts and creativity. Under the Indian Copyright Act, the author is recognized as a natural person who creates the work, whether it is literary, artistic, or musical and is considered the first owner of the copyright, with consideration to certain provisos. This distinction is crucial because copyright law traditionally acknowledges that only humans possess the cognitive ability to originate and express ideas creatively. However, this long-standing belief has been challenged by technological advancements, particularly by generative AI, which is raising ethical questions and

concerns in creative fields. AI blurs the line between originality and human intellect, making it difficult to determine whether a work produced with AI qualifies as original. Despite this, original expression remains the cornerstone of legal protection, forming the foundation of the economic and moral rights that allow authors to control and benefit from their creations.

The requirement that an author must be a natural person serves not only to recognize individual intellectual effort but also fulfils an essential legal function as when authorship is tied to a natural person, the law guarantees legal accountability and responsibility that can be properly assigned in cases of infringement, disputes, or liabilities related to the work. The creators of intellectual property are subject to legal frameworks governing their rights and responsibilities. When issues arise, whether related to ownership, copyright infringement, or attribution, the legal proceedings require a tangible individual against whom claims can be made, or from whom defences can be raised. If authorships were attributed to non-human entities, such as AI or corporations, this system would not function effectively. Legal entities, like companies, do not possess the inherent ability to create original works independently; they rely on the intellectual labour of individuals. If companies were considered authors, it would introduce significant challenges in assigning legal responsibility during accusations of IP infringement. Corporate entities do not have the same moral or intellectual accountability as individual authors. Moreover, legal accountability could become diluted if an organization with many employees or stakeholders were recognized as the author, making it difficult to identify the actual originator of the work or the person responsible for infringement. Furthermore, allowing companies to be considered authors would conflict with public policy, as it could lead to perpetual copyright protection for works, which would be detrimental to the public domain. While companies or corporate entities can hold copyright through assignment or ownership transfer, they cannot be considered the author of a work. Even when an individual creates a work as part of their employment within a company, the author remains the individual, although the company may hold the copyright by virtue of the employment contract.

COPYRIGHTABILITY OF AI-GENERATED WORKS

It seems counterintuitive to grant copyright protection to works generated by AI, but should this always be the rule? Is it fair to deny protection to any literary work simply because AI was involved in its creation? Current copyright law requires that a work possess some level of original expression to qualify for protection. However, consider a scenario where an author uses AI to correct grammar, refine their ideas, or simplify complex findings for the general public. In such cases, the core ideas and creativity still belong to the human author; AI merely assists with the presentation. Should these works be denied copyright protection simply because AI was a tool in the process? This raises the need for a more nuanced approach, evaluating each situation on a case-by-case basis to determine whether AI's contribution was significant enough to disqualify the work from protection. This is not a new challenge for IP laws, which have long dealt with the question of originality. Different countries already have varying standards for determining the originality of a work.

While it may seem logical to assume that the individual providing the prompts for AI is the creator of the resulting work, simply inputting a vague one-line prompt isn’t sufficient to meet the legal standards

for copyright protection even through the lens of the lowest thresholds for determination. Copyright is only granted if the work meets a threshold of originality and creativity. Though not recognized in India, *"sweat of the brow"* doctrine, awards copyright based on the effort and diligence an author puts into their work. It is to be highlighted that effort alone is not enough; there must be original intellectual input. A significant case for understanding originality in copyright law through sweat of brow is *University of London Press Ltd v. Tutorial Press Ltd.* In this case, a publisher compiled question papers issued by the University of London. The university claimed this was a violation of the copyright held by the professors who had invested their time and skill in creating those papers.

The publisher countered that the papers were derived from existing knowledge and thus lacked "originality" to qualify for copyright protection. However, the court ruled that despite drawing from existing knowledge, the effort and skill put into crafting the papers were sufficient to meet the threshold for originality, thereby making them eligible for copyright. This standard, which grants copyright based on diligence and effort rather than creativity, contrasts with the case of AI-generated work, where a simple prompt, regardless of how unique the output, lacks the human effort required for copyright protection. In India and most other jurisdictions, the use of AI complicates this determination, as courts and lawmakers will need to evaluate whether the AI-generated aspects of a work detract from its originality or merely assist in enhancing the author's original expression.

In the landmark case of *Eastern Book Company v. D.B. Modak*, Supreme Court Cases (SCC), a journal run by Eastern Book Company (EBC) since 1969, published Supreme Court judgments with additional elements like paragraph numbers, headnotes, formatting, and cross-references. In 2004, the respondents launched software containing judgments directly copied from SCC. EBC filed a copyright violation suit, claiming infringement of their original additions. The respondents argued that since government documents are not copyrightable, this principle should extend to judicial decisions, meaning SCC held no copyright over them. The Supreme Court of India herein examined different standards of "originality" to establish a benchmark for India. The court rejected the *sweat of the brow doctrine*, which grants copyright based solely on effort, as it felt this standard set the bar too low and unduly favoured the rights of the copyright holder. The court also considered the American *"modicum of creativity"* standard, which requires a minimum level of creativity for a work to be copyrightable. However, it found this standard too demanding. Instead, the court adopted the Canadian test, which focuses on the author's *"skill and judgment"*.

According to this test, the work must result from an author's application of skill and judgment, which should not be so trivial that it can be considered purely mechanical. This standard reinforces the notion that output generated by merely entering a single-line AI prompt cannot qualify for copyright protection. It was ultimately held that judicial decisions, in their edited and compiled form, involved the application of legal knowledge, skill, and judgment, making them eligible for copyright protection. By extension, this reasoning suggests that AI-generated works can also meet the originality threshold in India, provided that human skill and judgment were applied in creating the final product, regardless of whether the work was based on pre-existing knowledge. The court's decision reaches the understanding that while novelty may be too high a standard for copyright, the application of human

intellect remains a key factor in determining eligibility for protection, even in the context of AI-generated content.

Another test of originality is the "*Significant Input"* test which is the most appropriate test when it comes to the culmination of AI with copyright. Unlike rigid standards that require novelty or specific creative acts, this test allows for a flexible evaluation of the human contribution through skill, judgment, and effort. By focusing on the overall extent of human input, it ensures that copyright protection is only granted when the human element is substantial enough to make the final product fundamentally different or non-existent without it. This approach balances the evolving role of AI with the need to protect genuine human creativity. It outlines two key criteria for determining if an author using AI can claim copyright. *First*, it assesses whether there was any human involvement in the creation process. *Second*, it examines the extent of that involvement, requiring substantial human input through skill, judgment, and effort so that the final product would not exist or be fundamentally different without it. In the *Navigators Logistics Ltd. v. Kashif Qureshi* case, a copyright claim on a list generated by a computer was rejected due to a lack of human contribution, emphasizing that human involvement is essential for copyright protection in India.

In the U.S., a similar stance was taken in the *Zarya of the Dawn* case, where the U.S. Copyright Office (USCO) granted protection to a graphic novel created with AI-generated images. This was due to the significant human creativity involved in arranging and editing the AI images. The USCO formalized this approach, stating that AI-generated works may receive copyright protection if they include sufficient human authorship. Furthermore, the Copyright Office has stated it will "register an original work of authorship, provided that the work was created by a human being." This position is based on case law, such as *Feist Publications v Rural Telephone Service Company, Inc.*, which holds that copyright law only safeguards "the fruits of intellectual labour" grounded in human creativity. Similarly, in a recent Australian case, *Acohs Pty Ltd v Ucorp Pty Ltd.*, the court ruled that a work created with computer assistance could not be copyrighted because it was not produced by a human.

Though the *"Significant Input"* test shares similarities with the U.S. standard, it is broader and can be applied to various forms of creative work (music, books, software), not just graphic novels. It focuses on the overall level of human creativity, judgment, and effort, rather than specific acts like arranging or selecting AI-generated content. Lastly, the proposed test avoids using the U.S. "modicum of creativity" standard, which Indian courts find too stringent. Instead, it adheres to the "skill and judgment" test, ensuring that AI-generated works align with the Indian Copyright Act. After its amendment in 1994 to inculcate computer-generated works, including literary, dramatic, musical, or artistic works, Section 2(d)(v) was introduced in the act to define the authorship of such works as "the person who causes the work to be created." How the term "person" is defined and interpreted here becomes relevant, since as of now only natural persons have been recognised as authors under law. What therefore also needs to be clarified by the law and by the courts is the legal status of AI – whether AI can be defined as a 'person' under the law, and if so, to what extent. This approach helps Indian copyright law adapt to the growing influence of AI in creative industries.

The Case Study of Robust Artificially Intelligent Graphics and Art Visualizer (RAGHAV), which addresses the issue related to joint authorship of AI-Generated works in India. India initially became the first country to grant joint authorship to AI alongside the creator of the program. However, the Indian Copyright Office later expressed uncertainty about extending protection to AI-generated content, eventually issuing a withdrawal notice that revoked the co-authorship status granted to the AI alongside a natural person. RAGHAV, an AI painting application, created a painting titled 'Suryast,' which combined elements from Vincent van Gogh's 'Starry Night' and a photograph taken by Ankit Sahni for which the creator of RAGHAV filed two applications: one claiming sole authorship for the AI and another claiming joint authorship between the AI and Ankit Sahni.

In the wake of this case being pending with the Copyright office in India, a parliamentary Standing Committee on Commerce took up the issue in its 161st report, concluding that India's current copyright laws were inadequate to protect AI-generated works and recommended amendments to include such rights.

In 2020, Mr. Sahni applied to the USCO for copyright registration of 'Suryast,' listing both himself and RAGHAV as co-authors. He argued that the AI's contributions were distinct and independent from his own as the painting had been created by inputting his photograph into RAGHAV, along with Van Gogh's 'Starry Night' as the stylistic reference. However, the USCO initially rejected the application, emphasizing the lack of human involvement and authorship, stating that the human contribution could not be clearly separated from the final AI-generated work.

Mr. Sahni then filed a second request for reconsideration, arguing that RAGHAV was merely an assistive tool, and that the primary inputs, including the photograph and stylistic directions, were his. He also contended that the final work was not a derivative of Van Gogh's painting, as it was not substantially similar to the original. In response, the USCO reaffirmed its position that non-human creations are not eligible for copyright protection, and that human creativity must be evident in the final product. The office referenced its March 2023 guidance, which states that AI-generated works may be protected only if they are "essentially of human authorship" with the AI playing an assistive role. Applying this standard, the USCO concluded that while Sahni decided what elements to include, the AI tool was responsible for how those elements were incorporated, making RAGHAV the primary creative force.

Interestingly, Mr. Sahni successfully secured copyright registration for 'Suryast' in Canada, where only humans can be recognized as authors. He maintained that his creative process was so intertwined with RAGHAV's contributions that both should be considered joint authors under Canadian law. On the other hand. This raises two varying outcomes, therefore more upcoming case laws and legislations will be able to provide a concrete answer to the question of whether AI-generated works can be/ should be given protection or not and if yes, then to what extent.

LIABILITY FOR COPYRIGHT INFRINGEMENT: AI COMPANY VERSUS USER RESPONSIBILITY

AI developers' liability largely hinges on their 'Terms-of-Use.' If a developer claims ownership over the work generated by their AI, they may assert copyright unless another agreement is in place. However, most common AI models, including OpenAI, do not claim copyright over the generated outcomes. The creative product is the result of the user's application of thought, even though the AI provides substantial assistance in its creation. AI, including systems like ChatGPT, cannot own the content they generate, as they lack the legal personality required to be considered an author under U.S. and European copyright laws. When asked, ChatGPT itself has stated that content generated by it may or may not be protected by copyright, but it will not be owned by the AI. The risk of IP infringement is also significant because AI chatbots may generate content that infringes on IP rights by closely resembling or duplicating existing works, despite OpenAI's efforts to limit the use of copyright material in training models, publicly available data, including copyrighted material, is often used in AI training, raising questions about potential IP violations. Under OpenAI's Terms of Use, the user is ultimately responsible for the AI-generated output.

Copyright infringement cases focus on identifying the infringer, and users can be held liable for reproducing or creating derivative works that violate someone else's rights. Since AI models rely on existing content to generate new responses, the risk of copyright infringement is high. Legal action could be taken against both OpenAI and its users for unauthorized use of third-party content. In India, the Copyright Act was amended in 1994 to address computer-generated works, establishing that authorship belongs to the person who caused the work's creation. Based on this framework, the user is solely responsible for any copyright infringement, though ongoing court cases may further clarify the legal landscape in this area. The user, as the party who prompts and applies the AI's output, is considered the primary actor in copyright-related actions. If the AI generates content that infringes on another party's intellectual property rights—such as reproducing or deriving work from copyrighted material—the user may be held liable for violating reproduction or derivative work rights.

Ultimately, the responsibility for verifying the copyright status and accuracy of data generated by AI lies with the user. When individuals or organizations utilize AI tools, they must exercise due diligence in cross-checking the information provided against existing copyright protections and factual correctness. This involves ensuring that any AI-generated content does not infringe on the rights of copyright holders and is based on reliable sources. Users must be aware that while AI can assist in the creative process, it is their responsibility to critically evaluate and validate the output to mitigate the risk of copyright infringement or dissemination of false information. Thus, users play a crucial role in upholding intellectual property rights and ensuring the integrity of the content they produce.

Li Yunkai v. *Liu Yuanchun*

In November 2023, the Beijing Internet Court delivered a landmark ruling in a copyright infringement case involving an AI-generated image. The court addressed two critical questions: whether AI-generated works can be protected by copyright and, if so, who holds the copyright. The case involved a plaintiff who used the text-to-image generative AI model Stable Diffusion to create an image of a young woman. The plaintiff generated this image by entering various prompts and adjustments, later posting it on social media. The defendant subsequently used the image without permission, leading the

plaintiff to file a copyright infringement claim. The court examined the definition of "works" under the Copyright Law of the People's Republic of China, which mandates that copyrightable works must be original and reflect intellectual achievement. The court concluded that the plaintiff's detailed input and adjustments during the image creation process demonstrated significant intellectual contribution, thus qualifying the work as original. Furthermore, the court determined that originality, in this context, means that a work should reflect the author's subjective expression and not merely follow fixed procedures. The plaintiff's specific prompts and adjustments indicated their creative choices, leading the court to classify the image as a "work of fine arts" protected by copyright.

Regarding copyright ownership, the court clarified that copyright is owned by the author, who must be a natural or legal person. Since AI cannot qualify as an author, and given the plaintiff's substantial input in creating the image, the court awarded the copyright to the plaintiff. This ruling has significant implications for the future of AI and intellectual property in China, suggesting that courts may recognize the copyrightability of AI-generated works. The case highlights the importance of assessing each situation individually, considering the specifics of user input in generating content.

FAIR USE OR FAIR DEALING A POSSIBLE DEFENCE?

Thanks to the consumption of websites like YouTube, almost everyone is aware of the Section 52 of the Copyright Act, 1957, which provides specific exceptions to copyright infringement, allowing limited use of copyrighted material without the owner's authorization. The author wishes to explore into the idea whether this provision potentially defends the use of copyrighted content by AI tools, such as Large Language Models (LLMs). Though the law does not explicitly define "fair dealing," it permits the use of literary, dramatic, musical, or artistic works for purposes like research, private study, criticism, or review, which may not constitute infringement.

In India, the test for copyright infringement focuses on two key questions: whether the content is "substantially similar" to the original copyrighted work and whether it falls under the exceptions listed in Section 52. According to this framework, literary works generated by AI systems, such as LLMs, may not be considered infringement if used for private consumption, research, review, or educational purposes, as these uses typically fall within the exceptions outlined in the law. However, the situation changes when AI-generated content is used for commercial purposes or in ways that do not meet the exceptions. For example, if a person uses an LLM to generate a translation of a copyrighted book or to create an alternate ending to a novel and then publishes it under their own name, this will infringe the original author's copyright, as it goes beyond the scope of fair dealing.

Determining what qualifies as fair dealing ultimately rests with the courts, which evaluate each case based on the specific facts, circumstances, and established guidelines. Courts assess whether the use of the copyrighted material is justified within the context of the exceptions and whether the original work has been transformed in such a way that it constitutes an infringement. This legal standard is particularly relevant in cases involving AI, as the lines between creative input and replication of copyrighted material can sometimes blur, leading to potential infringement claims.

CONCLUSION

The normalization of AI in creative fields has been rapid, and the deeper issues that it presents remain largely unaddressed. What's even more unsettling is the fact that the creators of this technology admit that they cannot predict the full scope of challenges it may pose to humanity, with AI's unpredictability being one of its most concerning uncanny traits. There is an ongoing competition amongst the AI developing companies where they are blindly trying the create a model which can provide the broadest spectrum of services, negating even an ounce of thought towards the future implications of the same. It is a rat race where they are simply launching tech without even fully understanding it, which to say the least is very dangerous. Though AI may offer short-term profits for businesses, it threatens to displace human jobs, potentially leading to widespread unemployment and a host of social problems.

While generative AI can produce work based on user prompts, it's important to remember that it lacks original thought. These AI models rely on vast amounts of data, to generate their responses. Not only do they need historical data, but they also require up-to-date, protected content to provide the most relevant answers. OpenAI, an artificial intelligence research organization, with its most notable product being ChatGPT, declared that training AI models would be impossible without using copyrighted materials, since virtually all forms of human expression fall under copyright law, from blog posts and photographs to forum posts, bits of software code, and even government documents. This raises significant ethical issues, as companies using such data do so without necessarily obtaining consent from the original authors. Even if permissions were granted for AI training by the authors, does that give users the right to indirectly use the authors' work without acknowledgment? When an AI model like ChatGPT generates responses, it doesn't cite specific sources, making it difficult to trace the origins of the information. This blurring of intellectual property lines also raises questions about the accuracy and reliability of AI-generated content as it often draws from a mixture of wide range of data sources within its database. This concern is reflected by the disclaimers on AI platforms like in ChatGPT, which subtly warn users with statements like, *"ChatGPT can make mistakes. Check important info."*

The research paper has examined several key issues at the intersection of copyright law and AI, addressing integral questions about the future of intellectual property in the AI era. The first question explored whether works created using AI should be granted copyright protection. After an analysis of global legal standards, and Indian copyright regimes, the paper concludes that AI-generated works are not eligible for copyright protection, as current laws require a human author to exercise creativity, skill, and judgment. While AI can assist in the creation process, it lacks the legal personality and creative input necessary to be recognized as an author under existing frameworks. But this is not the thumb rule as works using AI but having considerable effort and creativity of the author or human input are up for protection given the stance of IP laws and the test of originality. While AI can assist in generating content, the core of copyright protection lies in human creativity, skill, and judgment. Without substantial human contribution, AI-generated works lack the originality required for copyright. Therefore, legal protection should not be extended to fully autonomous AI creations, but to works where human input plays a crucial role in shaping the final product. This approach ensures the protection of genuine creativity while acknowledging the evolving role of technology.

The second integral question investigated was whether AI or the user should bear liability for copyright infringement when copyrighted material is used through AI models. Although there is a lack of direct case law to provide definitive answers, this paper has drawn from existing legal principles and ongoing cases to offer a reasoned conclusion: users, rather than AI developers, are generally held responsible for any infringement because they initiate and control the use of AI-generated content. However, this remains an evolving area, and pending cases in jurisdictions such as the U.S. and Europe may soon offer clearer judicial guidance on this issue.

Another important topic, although not fully explored in this paper, is the issue of data mining. AI systems, particularly those like ChatGPT, rely on extensive data mining to train their algorithms, frequently using copyrighted material without clear authorization. This presents a significant and burgeoning legal question, particularly regarding fair use, data scraping, and privacy concerns. While this paper does not delve into that area, it is a fascinating issue that will likely grow in importance as AI technologies continue to develop and challenge traditional notions of intellectual property.

Ultimately, the research demonstrates that while AI's impact on copyright law is profound, the current legal frameworks remain centred on human authorship. Future court decisions and legislative changes will undoubtedly shape the path forward, but for now, the balance between innovation and the protection of creative rights remains focused on the human creator. The conclusions presented in this paper are drawn from the best available sources, even though some questions, such as liability for AI-generated content, remain unsettled pending further judicial decisions. This reflects the dynamic nature of the field, where continuous evolution and legal adaptation will be critical in addressing the challenges posed by AI.

*****

CYBER CRIME: LAW ENFORCEMENT AND PROCEDURAL CHALLENGE

Dr. Poonamdeep Kaur[19] and Prerna [20]

ABSTRACT

Cybersecurity has emerged as a major concern for people, businesses, and governmental entities, because of the growing need for digitalisation and the changing nature of cyber threats. This study explores the most recent developments in cybersecurity, such as the increase in phishing schemes, ransomware attacks, and the use of vulnerabilities in key infrastructures. The rising use of artificial intelligence (AI) and machine learning (ML) by cybercriminals to automate assaults and take advantage of system flaws is making these threats more complex. Predictive analytics, automated threat response, and anomaly detection are more defensive uses for AI and ML. Cybersecurity plans have become more complex due to the dynamic and ever-escalating conflict between cyber attackers and defenders brought about by these technologies. The Internet of Things (IoT) and cloud computing are growing at a rapid pace, which has increased the attack surface for hackers significantly in addition to AI-driven threats. Although they provide flexibility and scalability, cloud services come with hazards including data breaches and unauthorised access to private information. In a similar view, a lot of Internet of Things (IoT) devices lack strong security features, which leaves them open to widespread Distributed Denial of Service (DDoS) assaults and unapproved access. Therefore, protecting personal data, guaranteeing cyber resilience in essential infrastructures, and maintaining financial systems have become major priorities for all parties involved in the digital ecosystem. Concerns about the future are raised by the growing dependence on networked digital platforms, since vulnerabilities will grow if strict security measures are not implemented. Cybercrime continues to be a rising threat despite several preventive measures, and its global nature makes law enforcement operations more difficult. Because cyberspace is globalised, cybercriminals can operate internationally by taking advantage of legal frameworks that are out of date and regulatory inadequacies. To counter these dangers, legal measures like the General Data Protection Regulation (GDPR) in Europe and cybersecurity regulations in the US, China, and India have been implemented. To solve jurisdictional and enforcement difficulties, international coordination and flexible legal frameworks are necessary, as existing laws are unable to keep up with the fast evolution of cyberattacks. The enforcement of laws is complicated by jurisdictional overlaps and the absence of clear international agreements, necessitating coordinated international efforts to simplify legal responses. The most recent developments in cybersecurity strategies, methods, and future directions are also included in this study. For the purpose of identifying and automating responses to cyber threats, emerging developments in AI, ML and other advances are essential. The report emphasises how crucial it is for academics, decision-makers and business leaders to work together to create practical plans for handling the current state of cyberthreats. In order to secure information systems, preserve privacy and reduce threats in the future, it is imperative that cybersecurity measures be continuously adopted and that international efforts are coordinated.

INTRODUCTION

Cybercrime refers to illegal actions carried out via digital devices, networks or the internet. These crimes are difficult to control and prosecute because they frequently cross national borders. A significant international convention called the Budapest Convention on Cybercrime outlines a broad range of offences, such as financial fraud, cyberterrorism, hacking and data breaches. This wide scope

[19] Department of Laws, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, India.
[20] School of Law & Legal Studies, DAV University, Jalandhar, Punjab, India.

which targets not just individuals but also organizations and governments, underscores the complex nature of cybercrime.

The development in cybercrime in the twenty-first century has changed the criminal environment by presenting both opportunities and difficulties due to technical advancements. Any illegal activity involving computers, networks and the internet can be categorized as cybercrime. These crimes frequently cross international borders which presents difficult jurisdictional issues. The Budapest Convention on Cybercrime defines cybercrime as a broad category of offences that includes financial fraud, cyberterrorism, hacking, data breaches and child exploitation. This broad definition highlights the variety of hazards that cybercrime presents to governments, businesses and private citizens.

Growth of Cyber Crime

In recent decades, there has been an exponential increase in cybercrime, primarily due to the growing dependence on digital technology. INTERPOL estimates that in 2020, cyberattacks will have a global economic impact of more than $1 trillion. This growth is attributed to multiple factors:

1. Increased Internet Usage: As more people and companies move their operations online, cybersecurity vulnerabilities have expanded, giving thieves additional possibilities.
2. Technological Advancements: Cybercriminals now have a larger attack surface because to innovations like cloud computing, artificial intelligence, and the Internet of Things (IoT).
3. COVID-19 Pandemic: The widespread illness caused a sharp increase in ransomware attacks on vital industries including healthcare, which in turn caused a spike in cybercrime.

Impact of Cyber Crime

Cybercrime has a wide-ranging impact on various aspects of society, including:

1. Impact on the Economy: Cyberattacks cause large financial losses. Companies lose billions of dollars a year as a result of fraud, extortion and data breaches. Consequently, economies become unstable, operations become disrupted and reputations are harmed.
2. Social Impact: Identity theft, cyberbullying and cyberstalking victims frequently experience long-term psychological damage on a personal level. The adoption of new technologies is made more difficult by the erosion of public confidence in digital systems.
3. National Security: With the rise of cyberterrorism, cybercrime has become a serious threat to national security. Attacks against vital infrastructure, such financial institutions or energy systems, have the potential to destabilise entire countries and have a domino impact on world stability.

HISTORICAL EVOLUTION AND TRENDS

Cybercrime's origins may be traced back to the early days of computers, and its history is intimately linked to the advancement of digital technology. Cybercrime has become more sophisticated and sophisticated as technology has advanced, evolving from relatively basic acts of hacking to sophisticated, worldwide concerns that affect both the public and commercial sectors. Gaining

knowledge about the past development of cybercrime is essential to understanding its present patterns and potential future directions.

1. **Early Developments (1960s - 1980s):-**

The first large-scale computer systems appeared in the middle of the 20th century, sowing the seeds of cybercrime. In this time frame: Early hackers, frequently students and hobbyists, broke into computer systems in the 1960s and 1970s mostly out of curiosity and exploration rather than for financial gain. These early hacking techniques were mostly benign and aimed at testing the boundaries of computer technology. The first computer viruses appeared in the 1980s. For example, the 1982-discovered "Elk Cloner" virus was among the first known viruses to infect personal computers, despite its relative innocuous nature. Governments began recognizing the potential for malicious activities. In 1986, the U.S. passed the Computer Fraud and Abuse Act to address unauthorized access to computer systems, one of the earliest attempts to regulate cyber crime.

2. **The Rise of the Internet (1990s)**

With the development of the internet in the 1990s, cybercrime underwent a sea change in terms of reach and size. What started out as casual hacking or exploratory hacking soon turned into commercial hacking. Cybercriminals started making money by taking advantage of weaknesses in increasingly linked systems. An Overview The late 1990s saw a surge in online banking and e-commerce, which gave rise to crimes such as credit card fraud, identity theft, and internet frauds. During this time, phishing—a technique used to mislead people into. In 1995, the arrest of Kevin Mitnick, one of the most notorious early hackers, symbolized the growing seriousness of cyber crime. Mitnick's infiltration of major U.S. corporations demonstrated the economic impact and the national security risks posed by these crimes, disclosing financial and personal information—became very popular.

3. **Cybercrime's Globalisation in the 21st Century**

At the turn of the century, cybercrime became more widespread as the internet became a necessary tool for communication, trade, and day-to-day living: Illegal groups started taking use of the anonymity offered by the internet to carry out their illegal operations on a worldwide basis. These organisations were in charge of extensive financial fraud, drug trafficking, and even acts of terrorism, all of which were made possible by internet platforms. When the Dark Web first gained popularity in the early 2000s, it offered a covert, anonymous market for illegal goods and services, such as drugs, firearms, and data theft. The FBI closed down The Silk Road, one of the most notorious Dark Web marketplaces, in 2013, yet comparable websites still exist today. Viruses and worms are examples of malware attacks that have become increasingly complex. Millions of users worldwide were affected by the ILOVEYOU virus in 2000 and the Slammer worm in 2003, which showed how swiftly and destructively these attacks might spread. Over the last ten years, there has been a noticeable increase in ransomware assaults, in which hackers encrypt victims' data and demand payment to decrypt it. High-profile events like the 2017 WannaCry attack exposed the weaknesses of even vital infrastructure, devastating healthcare systems and businesses worldwide. States now frequently target other countries through cyber espionage and state-sponsored assaults in an effort to gain political, military, or economic leverage.

Examples include attacks on Ukraine's electricity grids and Russia's purported meddling in the 2016 US elections. The emergence of cryptocurrencies has given rise to new avenues for cybercriminals, particularly in fraud and money laundering. Cryptojacking has also proliferated, in which cybercriminals mine bitcoin using the computer power of their victims.

LAW ENFORCEMENT AGENCIES

India has recognised the growing necessity for specialised law enforcement organisations capable of addressing the increasing complexity of digital offences and has established a multi-layered approach to combat cyber crime. These organisations function at the federal, state, and municipal levels, each focussing on particular facets of cybercrime and making an effort to stay up with the swift advancements in both technology and criminal strategies. Nonetheless, issues with funding, coordination, and training continue to have an impact on the effectiveness of cybercrime enforcement nationwide.

Cyber Crime Investigation Cells

The establishment of Cyber Crime Investigation Cells (CCICs) is one of the most important aspects of India's cybercrime enforcement environment. These specialised cells are largely in charge of looking into and responding to offences relating to cyberspace, and they have been established in several states. Dealing with a wide range of crimes, including hacking, identity theft, online financial fraud, data breaches, and cyber harassment, is part of their work. Through the use of digital forensics, CCICs are able to track down cybercriminals using their electronic footprints, examine trends in data, and gather proof for court cases. But in spite of their significance, many CCICs face obstacles like inadequate technology resources, a shortage of skilled staff, and lengthy legal procedural bureaucracy. Some states, such as Maharashtra, have led the way in developing well-equipped and efficient cybercrime units, but this degree of expertise is not shared by all regions.

The Indian Computer Emergency Response Team

At the national level, the Indian Computer Emergency Response Team serves as the key agency for responding to cybersecurity incidents. CERT-In, which reports to the Ministry of Electronics and Information Technology, is in charge of monitoring cybersecurity risks, issuing alerts, and coordinating responses to large-scale cyber attacks on vital infrastructure. This covers situations like ransomware assaults, denial of service (DoS) attacks, and data breaches, which can affect both the public and commercial sectors. CERT-In has played an important role in mitigating high-profile cyber threats, such as the WannaCry ransomware outbreak, which impacted many organisations and institutions in India. In addition to responding to incidents, CERT-In collaborates with both domestic and foreign organisations to combat cybercrime, which is critical given the global nature of digital threats.

The National Cyber Crime Reporting Portal

The National Cyber Crime Reporting Portal has strengthened India's ability to tackle cybercrime by providing a centralised, easily accessible platform for victims to report cybercrimes. This portal, which is part of the government's Cyber Crime Prevention against Women and Children (CCPWC) project, allows anyone, even anonymous users, to file complaints online regarding sensitive subjects such as

cyber harassment, cyberstalking, and revenge pornography. By making it simple for victims to report crimes, the portal reduces the hesitation that sometimes comes with traditional police reporting, especially in cases involving personal and financial harm. Once a complaint is filed, it is forwarded to the appropriate state or national agencies for investigation, resulting in a faster and more coordinated response.

In addition to national efforts, numerous states have made substantial headway in establishing cyber police stations and state-level cybercrime units. These specialised police stations only handle cybercrime cases, with trained officers and forensic professionals focussing on internet scams, hacking, and social media offences. For example, Maharashtra's cyber police deal with hundreds of cases per year, ranging from high-profile corporate espionage to internet harassment and identity theft. Similarly, Delhi's Cyber Crime Unit has achieved tremendous progress in combating cyberstalking, financial fraud, and crimes against women, underscoring the importance of gender-sensitive methods to cybercrime enforcement. These state-level initiatives are critical because they address region-specific cyber risks while reducing the pressure on overburdened national agencies.

While certain states, such as Maharashtra, Karnataka, and Telangana, have established more modern cybercrime units, India's overall cyber law enforcement landscape remains unequal. Many jurisdictions still lack appropriate resources and skilled personnel, limiting their ability to combat increasingly complex cybercrimes. The challenges of under-resourced cybercrime cells, as well as the lack of suitable legislative and technical frameworks in some places, provide weaknesses for cybercriminals to exploit. Furthermore, the necessity for ongoing capacity-building programs and training workshops is critical, as law enforcement agents must stay current on the latest technology and cybercrime tactics.

DATA BREACHES IN AUSTRALIA

In December 2022, Australia faced a significant data breach involving Medibank, which affected around 9.7 million customers. The breach was orchestrated by the ransomware group REvil, believed to be linked to Russian cybercriminals. Sensitive data, including medical records, passport numbers, and birthdates, was leaked. Medibank opted not to pay the ransom, and the stolen data was reportedly made available on the dark web. While there were no immediate reports of financial fraud, authorities advised customers to remain vigilant regarding their personal information.

Also, The Optus data breach, which occurred in September 2022, is one of Australia's largest cyber incidents, affecting approximately 10 million customers. The breach involved unauthorized access to sensitive customer information, including names, dates of birth, phone numbers, email addresses, and, in some cases, driver's license and passport numbers.

The breach was allegedly carried out by a hacker who claimed to have accessed Optus' systems and offered to sell the stolen data on dark web forums. The attack raised significant concerns about Optus' data security practices and prompted investigations by the Australian Federal Police (AFP) and the Office of the Australian Information Commissioner (OAIC).

In response to the breach, Optus implemented several measures to enhance security and offered affected customers support, including credit monitoring services. The incident sparked discussions on the need

for stronger regulatory frameworks and cybersecurity measures across the telecommunications sector to protect consumer data more effectively.

CHALLENGES IN CYBER LAW ENFORCEMENT

India's law enforcement agencies are facing a variety of challenges when dealing with cyber crime, largely due to the dynamic and evolving nature of technology. Cybercriminals are constantly refining their tactics, making it difficult for the existing legal and enforcement frameworks to keep pace. These challenges are not just technical but also involve issues related to jurisdiction, capacity, and international cooperation. Below is an in-depth exploration of some of the primary challenges.

Technological Challenges

One of the most serious barriers to executing cyber laws in India is the presence of technological gaps among law enforcement authorities. As cybercriminals increasingly use modern technologies like AI and machine learning to automate assaults, exploit system weaknesses, and build sophisticated phishing schemes, many Indian law enforcement agencies struggle to keep up with the changes. They are unable to properly combat and investigate cybercrime because they lack access to cutting-edge technologies and tools.

- *Outdated Tools and Resources:* Many cybercrime units, particularly at the state level, rely on out-of-date software and forensic tools that are insufficient to combat complex cyber threats such as ransomware, Distributed Denial of Service (DDoS) attacks, and deepfake technologies. The lack of contemporary encryption-breaking technologies and data recovery processes limits investigators' capacity to collect key evidence from encrypted devices and networks, stalling investigations and resulting in incomplete data retrieval.
- *Limited Expertise:* As technology advances in cybercrime, law enforcement officials must keep their skill sets current. However, many units lack individuals with specialised knowledge in fields such as ethical hacking, network forensics, and virus analysis. In many circumstances, police personnel and investigators are not given appropriate training on the latest digital forensics technologies, AI-driven malware, or cloud-based criminal operations, further widening the gap between cybercriminals and law enforcement.
- *Inadequate equipment:* Aside from outmoded tools, many cybercrime cells work in conditions that lack the required equipment to conduct advanced cyber investigations. For example, some states' digital forensic labs may not have enough processing power to analyse enormous amounts of data, or they may lack the required cybersecurity safeguards to protect sensitive information during investigations.
- *IoT and Cloud Vulnerabilities:* With the advent of the Internet of Things (IoT) and cloud computing, the cyber attack surface has grown rapidly. Many IoT devices lack effective security safeguards, making it difficult for law enforcement agencies to secure and investigate crimes involving them. Similarly, cloud storage complicates data retrieval across borders

because some servers are located in nations other than India. The inability to quickly access and secure cloud data leaves investigators hamstrung in time-sensitive cases.

Judicial Challenges

Fragmented Legal Framework: In India, cybercrime is largely punished under the Information Technology Act of 2000, which offers a legal framework for dealing with offences such as hacking, identity theft, and data breach. However, the reach of the IT Act is limited to Indian borders, making it impossible to prosecute criminals stationed abroad. Furthermore, the lack of an internationally harmonised legal framework for cybercrime creates gaps that cybercriminals might exploit.

Extraterritorial Jurisdiction: While Indian law enforcement has the authority to pursue cyber offences affecting the country under the IT Act's extraterritorial jurisdiction clauses, applying these laws is difficult in practice. Requests for cooperation from foreign governments, particularly in acquiring digital evidence, are frequently delayed or ignored due to bureaucratic red tape, different legal systems, and competing agendas. Even when Indian police have identified the culprits of cybercrimes, extradition can be a lengthy and complicated process, further delaying justice.

Other Challenges

1. **Complexity in Obtaining Digital Evidence:-** It is challenging to gather digital evidence in a way that is legally admissible in court because of the nature of cybercrime. In contrast to physical crimes, where concrete evidence may be found at the scene of the crime, cybercrime investigations frequently need access to data that is held in many locations, such as encrypted platforms or foreign servers. The formalities involved in requesting access to such data might be cumbersome and impede prompt prosecution, particularly if the data is kept outside of India. Due to legal or procedural obstacles, law enforcement organisations frequently experience delays in receiving evidence from service providers, both domestically and internationally.

2. **Chain of Custody for Digital Evidence:-** In cybercrime investigations, keeping an appropriate chain of custody for digital evidence is essential to prevent tampering, but it is also one of the most difficult tasks. If not adequately secured, digital evidence—such as emails, logs, or malware—can be quickly changed or erased. In India, protocols for the management, preservation, and exhibition of digital evidence are still developing. Technological and knowledge deficiencies may give rise to procedural inaccuracies, rendering evidence inadmissible in court. It's possible that law enforcement personnel lack the necessary training to preserve the integrity of digital evidence while conducting investigations.

3. **Slow and Complex Mutual Legal Assistance Treaties (MLATs):-** When cybercrimes involve perpetrators or servers located outside India, law enforcement agencies must often rely on Mutual Legal Assistance Treaties (MLATs) to obtain evidence or extradite suspects. These treaties are slow and bureaucratic, often taking months or even years to process, which significantly hinders timely investigations. Cybercrimes, by their nature, evolve quickly, and this procedural delay makes it difficult for investigators to act within the necessary timeframes. The legal process for requesting cross-border cooperation is lengthy, often resulting in lost evidence or suspects fleeing jurisdiction.

4. Lack of Standard Operating Procedures (SOPs):- Cybercrime investigations across different states and jurisdictions in India often suffer from inconsistencies due to the lack of standardized operating procedures (SOPs) for cybercrime cases. This leads to different approaches in handling similar cases, causing inefficiencies and delays. The absence of a national framework for cybercrime investigation procedures, from data collection to prosecution, results in cases being handled differently across regions. For instance, some states may have more advanced cybercrime cells with updated forensic labs, while others lack the basic infrastructure, resulting in uneven enforcement.

5. Prolonged Judicial Procedures:- Even when law enforcement successfully gathers evidence and arrests suspects, the judicial process in India is often slow. Cybercrime cases can take years to proceed through the courts due to procedural delays, backlog of cases, and the lack of specialized knowledge among judicial officers. The absence of fast-track courts specifically for cybercrime means that cases are subject to the same delays as other criminal matters, leading to long waits for justice. Furthermore, many judges are not adequately trained in understanding the technicalities of cybercrime, which complicates the prosecution process.

6. Procedural Gaps in International Cooperation:- Cybercrime is a worldwide phenomenon by definition, and procedural challenges frequently arise when international cooperation is required. While India has signed various international treaties, there is still a lack of smooth coordination between Indian officials and their overseas counterparts. The bureaucratic structure of foreign law enforcement cooperation causes delays in transmitting intelligence, evidence, and suspect information. Furthermore, disparities in cybercrime legislation and data privacy standards between nations present further procedural challenges for Indian law enforcement organisations seeking information from international firms.

7. Limited Use of Cybercrime Legislation:- Although India has laws to combat cybercrime, such as the Information Technology Act (2000), procedural gaps frequently arise when applying these laws to new and growing types of cybercrime. For example, many crimes involving AI-driven assaults, ransomware, or IoT vulnerabilities are not specifically covered by existing legislation, creating procedural confusion on how to address such instances. Furthermore, cyber laws in India are not always clear, causing delays in prosecution as courts try to interpret and apply outdated or unclear legislation to modern cybercrime scenarios.

The procedural hurdles in cyber law enforcement in India include difficulties in gathering, preserving, and presenting digital evidence, sluggish international collaboration, inconsistencies in investigative techniques, and lengthy judicial processes. To improve the effectiveness of cybercrime investigations, clearer guidelines, speedier legal frameworks, and greater cross-border collaboration will be required.

SUGGESTIONS AND CONCLUSION

1. Law enforcement organisations must be armed with cutting-edge forensic techniques, such as artificial intelligence (AI) and machine learning (ML). These tools would improve the ability to monitor cybercriminal activity, decipher encrypted data, and analyse blockchain networks.

2. Law enforcement personnel, especially judicial officials, should get specialised training in digital forensics and cyber investigations as part of ongoing professional development programs. Such training will help them to keep up with the changing nature of cybercrime.

3. The government should establish a set of thorough Standard Operating Procedures (SOPs) that apply to all cybercrime investigations across countries. This would standardise investigative procedures, assuring a consistent approach to the gathering, preservation, and presentation of digital evidence. The creation of dedicated cybercrime courts or a fast-track method for adjudicating cybercrime cases would shorten delays and assure swift justice. Also considering technical nature of cybercrime, specialised courts are required for effective judicial processes.

4. A concerted national campaign should be launched to raise public awareness of cyber risks, prevention measures, and reporting procedures. Such programs would help to address the issue of underreporting by encouraging residents to actively engage with law enforcement organisations.

5. India must prioritise the negotiation of more effective Mutual Legal Assistance Treaties (MLATs) to speed up evidence exchange and cross-border extradition of cybercriminals. Streamlined legal collaboration with other countries is critical in combating cybercrime's international nature.

6. India must prioritise the negotiation of more effective Mutual Legal Assistance Treaties (MLATs) to speed up evidence exchange and cross-border extradition of cybercriminals. Streamlined legal collaboration with other countries is critical in combating cybercrime's international nature.The development of dedicated legal standards for the prosecution of new-age cybercrimes will give clarity in legal interpretation and application, improving the efficiency of judicial proceedings in cybercrime matters.

7. Collaboration between government agencies and private enterprises, particularly in technology, finance, and cybersecurity, should be promoted. This cooperation would allow law enforcement and industry parties to share intelligence, technical expertise, and resources to their mutual benefit.

This study report investigated the varied environment of cybercrime in India, emphasising the enormous problems that law enforcement agencies face in combating this expanding menace. As technology advances at an unprecedented rate, the nature of cybercrime has changed, posing new difficulties that necessitate a comprehensive and adaptable response. Despite regulatory frameworks such as the Information Technology Act of 2000 and continuous efforts to improve cybercrime units, procedural challenges exist. Key difficulties include the challenges of digital evidence collecting, jurisdictional ambiguities, and insufficient training for law enforcement personnel. These problems not only impede timely and effective investigations, but they also have an impact on overall cybercrime conviction rates. Addressing these issues will need a collaborative effort from all stakeholders, including government agencies, law enforcement, and the general public. By fostering a proactive, collaborative, and informed approach to cybercrime enforcement, India can enhance its capacity to respond effectively to this evolving threat, ensuring the safety and security of its digital landscape.

*****

AI AND FACE-MAPPING TECHNIQUES IN LAW ENFORCEMENT: NAVIGATING PROCEDURAL AND ETHICAL CHALLENGES

Nandana Rajesh[21]

ABSTRACT

Artificial Intelligence (AI) and face-mapping technologies are reshaping law enforcement by offering innovative tools for identifying individuals and solving crimes. These systems enable rapid, real-time facial recognition, contributing to enhanced public safety through the identification of suspects, prevention of criminal activities, and locating missing persons. However, the adoption of such technologies raises significant procedural, ethical, and legal concerns. This paper aims to critically assess the impact of AI-based face-mapping on fundamental rights such as privacy and due process. It investigates the potential for algorithmic bias, surveillance overreach, and wrongful identification, especially among marginalized communities. The primary objective of this study is to explore the procedural challenges and risks associated with the use of AI-driven face-mapping in law enforcement. It aims to evaluate the legal frameworks currently governing AI and facial recognition in various jurisdictions, identify gaps in existing laws that could lead to privacy violations or breaches of due process and propose guidelines for the ethical and transparent use of AI in law enforcement, balancing security and human rights. The paper adopts a qualitative research methodology, utilizing a comparative analysis of international and national legal instruments governing AI in law enforcement. The study draws on case law, policy papers, and academic literature to assess the effectiveness of current regulations. Through interviews with legal experts and law enforcement professionals, it also examines the practical challenges faced in the implementation of these technologies. By addressing both the promises and perils of AI in facial recognition, the paper seeks to contribute to the growing discourse on creating a balanced regulatory framework that ensures security without compromising civil liberties.

Keywords: AI, Face-mapping, Law enforcement, Privacy, Procedural challenges, Civil liberties.

INTRODUCTION

The continuous advancement of artificial intelligence as well as its applications in law enforcement, particularly face-mapping and facial recognition technologies, has made a revolution in crime prevention, suspect identification, and overall public safety strategies. AI-based facial recognition systems enables law enforcement agencies to process vast amounts of biometric data, identifying individuals with remarkable speed and precision. However, while these technologies provide undeniable advantages, they also present a host of legal, procedural, and ethical challenges that demand careful scrutiny.

This paper examines the use of AI and face-mapping technologies in law enforcement, addressing the procedural challenges associated with their implementation, the ethical dilemmas they pose, and their broader human rights implications. As AI continues to influence policing practices globally, understanding these challenges is crucial to ensuring that the deployment of such technologies is responsible, transparent, and adheres to the rule of law.

[21] Research Scholar at School of Legal Studies, CUSAT, India.

THE ROLE OF AI AND FACE-MAPPING IN LAW ENFORCEMENT

AI-powered facial recognition systems are increasingly being incorporated into law enforcement for various purposes, such as identifying suspects, tracking criminals, and enhancing border security. These systems utilize machine learning algorithms that analyze facial features to match them against large databases, thus providing law enforcement with a powerful tool for identifying individuals in real-time.

Face-mapping technology involves the creation of detailed 3D models of human faces, capturing unique biometric markers such as the distance between eyes, nose, and mouth, as well as skin texture. AI processes this data to create accurate digital representations, which can be compared with stored images for identification purposes. The technology can operate in both static and dynamic environments, with applications ranging from scanning ID photos to analyzing live surveillance footage.

The potential benefits of AI and face-mapping in law enforcement are significant. These technologies can streamline investigations, enhance efficiency in crime prevention, and support the accurate identification of suspects. In instances such as locating missing persons or apprehending dangerous criminals, AI-driven facial recognition can be invaluable. However, this rise in efficiency must be weighed against the procedural and ethical challenges posed by these technologies.

PROCEDURAL CHALLENGES

While AI-based facial recognition systems promise enhanced law enforcement capabilities, their deployment raises several critical procedural challenges that must be addressed to protect the integrity of justice systems.

1. Accuracy and Reliability

One of the most significant concerns surrounding facial recognition technology is its accuracy. Despite advancements in AI, face-mapping algorithms are not infallible. Studies have shown that these systems can misidentify individuals, particularly when the dataset they are trained on is biased or incomplete. Misidentifications can result in wrongful arrests, unwarranted searches, and reputational damage to innocent individuals. For example, the National Institute of Standards and Technology (NIST) found that facial recognition systems used by U.S. law enforcement exhibited higher error rates when identifying African Americans, women, and younger individuals.

The reliance on facial recognition technologies in criminal investigations raises serious questions about procedural fairness. Wrongful identification could lead to the violation of the principle of *innocent until proven guilty* which is a cornerstone of modern legal systems. Furthermore, individuals misidentified by AI systems may face significant difficulties in proving their innocence, as human oversight in these technologies is often limited.

2. Bias in Algorithms

Bias within AI algorithms is a profound procedural challenge. Facial recognition systems are often trained on datasets that lack diversity, leading to disproportionate impacts on marginalized groups. Research has indicated that facial recognition technology performs poorly in identifying people of colour, women, and non-binary individuals, creating a discriminatory effect in law enforcement

practices. This bias can manifest in wrongful arrests and higher surveillance of minority communities, perpetuating systemic inequalities in the criminal justice system.

The implications of algorithmic bias extend beyond misidentification; they challenge the ethical foundations of law enforcement. Law enforcement agencies have a duty to uphold the principle of non-discrimination, as enshrined in various human rights instruments. Biased algorithms undermine this duty and erode public trust in policing institutions.

3. Admissibility of AI-Generated Evidence

Another procedural issue relates to the admissibility of AI-generated evidence in court. Facial recognition technology is often perceived as objective and neutral, but the opaque nature of AI decision-making processes complicates its use as admissible evidence. Courts may struggle to determine whether AI-generated evidence is reliable and whether the process behind it adheres to established standards of fairness and transparency.

Furthermore, the lack of legal clarity around the admissibility of AI-generated evidence creates a risk that this technology could be used without adequate judicial oversight. Questions around how facial recognition data is collected, stored, and analyzed must be addressed to ensure that such evidence is used appropriately and does not compromise defendants' rights to a fair trial.

4. Lack of Comprehensive Legal Frameworks

One of the most pressing procedural challenges is the absence of a comprehensive legal framework that is regulating AI and facial recognition technologies. Many jurisdictions lack specific laws governing the use of AI in law enforcement, creating a legal vacuum that leaves room for potential abuses of power. Without robust regulations, there is little oversight or accountability for the use of facial recognition technology, allowing law enforcement agencies to operate with minimal constraints.

Moreover, the absence of uniform international standards governing AI and face-mapping technologies complicates cross-border law enforcement efforts. The development of international norms that align the use of AI in law enforcement with human rights obligations is essential to ensuring that these technologies are used responsibly.

ETHICAL CONCERNS

The ethical concerns associated with the use of AI and face-mapping technologies in law enforcement are equally significant. These technologies raise questions about privacy, consent, transparency, and accountability, all of which are central to the ethical governance of emerging technologies.

1. Privacy and Surveillance

AI-driven facial recognition systems enable law enforcement agencies to conduct widespread surveillance, often without the knowledge or consent of individuals being monitored. The ability of these technologies to operate in public spaces creates a pervasive surveillance environment that risks infringing on individuals' right to privacy. In countries with limited data protection regulations, this threat is even more pronounced.

Mass surveillance, enabled by facial recognition, can have chilling effects on the exercise of fundamental rights such as freedom of assembly and freedom of expression. Individuals may feel inhibited from participating in public protests or engaging in lawful dissent if they fear being constantly monitored by AI systems.

2. Transparency and Accountability

The opaque nature of AI systems presents a significant ethical dilemma. Unlike traditional policing methods, which involve human officers whose actions can be scrutinized and questioned, AI systems operate as "black boxes," making it difficult to understand how decisions are made. This lack of transparency undermines accountability, as individuals affected by AI-driven decisions often have no means of challenging or understanding the reasoning behind those decisions.

Accountability is further complicated by the absence of human oversight in many AI systems. Law enforcement agencies must ensure that AI systems are used under human supervision, with clear channels for reviewing and correcting errors. Without human oversight, the potential for AI to perpetuate unjust outcomes increases, as algorithms can make decisions with significant consequences for individuals' lives and liberties.

3. Informed Consent and Autonomy

The deployment of facial recognition technologies often occurs without individuals' knowledge or consent, raising ethical concerns about autonomy and the right to control one's personal information. In many cases, individuals are unaware that their facial data is being collected, stored, and analyzed, violating their right to informed consent.

The collection of biometric data without consent is particularly problematic in democratic societies, where the protection of individual autonomy is a fundamental value. Law enforcement agencies must strike a balance between using advanced technologies for public safety and respecting the rights of individuals to control their own biometric information.

HUMAN RIGHTS IMPLICATIONS

The use of AI and face-mapping technologies in law enforcement intersects with various human rights issues, particularly those related to privacy, non-discrimination, and the right to a fair trial.

1. Right to Privacy

The right to privacy is enshrined in numerous international human rights instruments, including Article 17 of the International Covenant on Civil and Political Rights (ICCPR). AI-driven surveillance systems, which rely on the collection and analysis of vast amounts of personal data, pose a significant threat to this right. The indiscriminate collection of biometric data, combined with the ability to track individuals' movements and activities, creates a surveillance apparatus that infringes on individuals' right to live free from unwarranted intrusion.

2. Non-Discrimination

AI systems that exhibit bias in identifying certain demographic groups risk violating the right to non-discrimination. Discriminatory practices in law enforcement can disproportionately affect marginalized communities, leading to higher rates of surveillance, arrests, and criminal charges. International human rights law, including the Universal Declaration of Human Rights (UDHR), prohibits discrimination on the basis of race, gender, or other protected characteristics. AI systems that perpetuate such discrimination violate these legal norms and undermine efforts to promote equality in the criminal justice system.

3. Right to a Fair Trial

The use of facial recognition technology in law enforcement can also impact the right to a fair trial, as guaranteed by Article 14 of the ICCPR. When AI-generated evidence is used in court without sufficient oversight or transparency, defendants may be denied the opportunity to challenge the validity of the evidence against them. Ensuring that AI-generated evidence is subject to the same standards of scrutiny as other forms of evidence is critical to protecting the right to a fair trial.

RECOMMENDATIONS

To address the procedural and ethical challenges posed by AI and face-mapping technologies, robust regulatory frameworks are needed at both the national and international levels. Key recommendations include:

1. Legal Safeguards

Governments must enact legal safeguards to regulate the use of AI in law enforcement. These safeguards should include clear guidelines on data collection, storage, and use, ensuring that individuals' privacy rights are protected. Furthermore, law enforcement agencies must be required to obtain warrants or other legal authorizations before using facial recognition technology in certain contexts, such as during public demonstrations.

2. Human Oversight

AI systems should never operate without human oversight, particularly in high-stakes situations such as criminal investigations. Human officers must retain the final decision-making authority, ensuring that AI tools are used as support mechanisms rather than as autonomous decision-makers. The involvement of human oversight is crucial to mitigating the risks of errors, bias, and injustice.

3. Algorithm Audits and Bias Mitigation

Regular audits of AI algorithms are necessary to identify and correct biases. Auditing processes should involve independent experts and civil society organizations to ensure transparency and accountability. Additionally, AI developers must prioritize the use of diverse datasets to train facial recognition systems, reducing the likelihood of bias in law enforcement applications.

4. International Norms

The development of international legal standards is essential for regulating the cross-border use of AI

in law enforcement. International human rights bodies should work together to establish guidelines that harmonize the use of facial recognition technologies with global human rights obligations. These guidelines should prioritize transparency, accountability, and the protection of fundamental rights.

CONCLUSION

AI and face-mapping technologies have the potential to revolutionize law enforcement, offering unprecedented efficiency and accuracy in criminal investigations. However, their deployment must be carefully managed to avoid infringing on individuals' rights and liberties. The procedural and ethical challenges posed by AI, including issues of bias, privacy, transparency, and accountability, require urgent attention from policymakers, legal experts, and human rights advocates.

As AI continues to shape the future of policing, it is essential to strike a balance between technological innovation and the protection of fundamental rights. By developing robust legal frameworks, ensuring human oversight, and promoting transparency, societies can harness the benefits of AI while safeguarding justice, fairness, and equality for all.

*****

ROLE OF POLICE IN INVESTIGATING DIGITAL CRIMES

Siddharth Baskar[22]

ABSTRACT

The development of technology and the improvement of connectivity have made it easier to share information and provide services; however, they also present a significant challenge because of the increased vulnerability to the escalation of digital crimes on a global scale. Increasing public awareness and protecting citizens from the dangers of digital crimes are two of the most important roles that the police play. As a crucial framework for protecting individuals and imposing substantial penalties on wrongdoers for their misconduct, the Information Technology Act of 2000 ("IT Act") serves as a crucial framework. The law enforcement agencies need to work together with cybersecurity experts from both the national and international levels to enhance their capabilities in dealing with the negative effects of cybercrime. The role of law enforcement in investigating digital crimes is becoming increasingly important because of the rise in the number of digital crimes. The purpose of this research is to investigate the responsibilities that are necessary to combat cyber-crimes in the digital realm. With the help of this study, we hope to gain a better understanding of the role that law enforcement plays in protecting cyberspace from digital offences. This places an emphasis on understanding the legal framework, incorporating recommendations, and case study analysis to determine the factors that lead individuals to become victims of digital crimes.

Keywords: Digital Space, Cyber Crime, Information Technology Act, Law Enforcement.

INTRODUCTION

Fraud, theft, mischief, forgery, defamation, stealing, cyber harassment, and similar offences perpetrated via cyberspace (any electronic device) with the intent to cause substantial harm to others constitute digital crime. Increase of cybercrime has incentivized criminal activities, cyber criminals are being paid for stealing credit card information's, email accounts of individuals. The significance of cybercrime investigations and the role of law in regulation is paramount. A pertinent inquiry that arises now is how cyber policing is conducted.

The Information Technology Act of 2008 explicitly delineates Sections 78 and 80, which empower police officers to conduct searches, enter premises, inspect, and make arrests without a warrant if they possess reasonable suspicion of an offence being committed or about to be committed under the Act. The efficacy of digital crime investigations is contingent upon the officers overseeing them, necessitating the recruitment of the most qualified individuals in the field of cyber-crime technology to mitigate potential threats. The Supreme Court of India, in the case of *Prakash Singh and Ors. v. Union of India*, has mandated the establishment of specialised investigative police, distinct from law enforcement agencies, to facilitate more effective dispute resolution. Numerous legislations, including the *Model Police Act of 2006*, also stipulate such measures. It is essential that digital crimes are investigated comprehensively, necessitating a specialised team to effectively combat cyber-crimes in the digital realm.

[22] Assistant Professor at IILM University, Gurgaon, India.

COMBATTING CYBER CRIMES

Indian legislation mandates cyber policing, which is essential for addressing cyber-crimes. "*Section 69 of the IT Act authorises the government and its agencies to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource, contingent upon adherence to the established procedures*." This authority may be exercised if the Central or State Government considers it necessary or beneficial for the preservation of India's sovereignty or integrity, national defence, state security, diplomatic relations, public order, or to prevent incitement to any cognisable offence or for the investigation of any crime.

The "*Budapest Convention*," which came into effect in 2004, addresses cyber-crimes in the international context and recommends the integration of safety mechanisms into the domestic laws of nations. Regrettably, the convention has not garnered international approval, and India has also dismissed it on the grounds that it was absent during the draughting process, which may infringe upon India's sovereignty.

Taking into consideration this convention, I believe it is of the utmost importance to recognise that the state is not the sole protector of cyber policing. Corporations and non-governmental organisations (NGOs) should be given the responsibility of addressing cybercrimes. These organisations should be able to obtain prior approval from the government to leverage their expertise in strengthening security mechanisms. This will result in the creation of an environment that supports justice and serves as a deterrent for individuals who commit such offences. Criminals who commit such offences may operate in several different jurisdictions, such as different countries. An international convention that is supported by the international community could serve as a norm that is legally binding to punish those who commit such offences.

CYBER CRIME INVESTIGATION

Given the rise in cyber-crimes, it is imperative to establish effective mechanisms, as investigation is crucial for holding perpetrators accountable for their offences. A functional model for cybercrime investigations is essential, and I believe it is necessary to integrate the following elements to combat cybercrime effectively.

To reduce the likelihood of cross-contamination, it is essential to have a thorough understanding of the procedures for gathering evidence and how it will be utilised, as well as the processes for storing evidence. In the case of recovering data that has been deleted, for example, the examination of evidence pertains to recover the data. To ensure that investigations into cybercrime are carried out without any interruptions and to guarantee that compliance is achieved, these methods need to be integrated.

CASE STUDY

The purpose of the case study is to bring attention to the fact that it is essential for individuals to increase their awareness of the cybercrimes that are currently occurring in our society. Because cybercrimes are

not limited by jurisdictional boundaries, it is imperative that efforts be made to cultivate an environment that is robust in terms of cyber security.

Case study – 1

The WannaCry Ransomware Attack: In 2017, a global cyber assault targeted systems running on Microsoft Windows, encrypting files and demanding a ransom for their release. The attack significantly affected over 100 countries and organisations, including Honda, FedEx, and Nissan. The solution was initiated by security researcher Marcus Hutchins, who released emergency security patches and collaborated with cybersecurity firms to eliminate the worm. Consequently, extensive systems that were impacted had to either pay a ransom to decrypt their files or await security patches to address the vulnerability.

It is essential to acknowledge that we were not adequately prepared to deal with this ransomware. For this reason, I believe that we require the assistance of cybersecurity companies that collaborate with the government and engage in cyber policing, which has the potential to reduce the severity of such impacts on a global scale. It is imperative that we take immediate action to bring about a change in our laws and integrate the work of cyber security firms with the work of the government.

Case Study - 2

Remote Access Trojan ("RAT") A schoolteacher named Aisha inadvertently downloaded a malware Remote Access Trojan ("RAT") onto her smartphone. The malware compromised Aisha's phone, granting the cybercriminal access to her email and text messages, which were subsequently disseminated to her colleagues and family members. The images were digitally manipulated ("deepfakes") and uploaded to pornographic websites. This case highlights the necessity of promptly reporting such crimes to cyber security units; however, Aisha initially failed to report the incident to the police and instead attempted to trace the websites where the images were disseminated. The Australian Police subsequently acknowledged the case and resolved the issue.

Case Study 3 -

Yahoo Data Breach – The Yahoo data breach involved cyber attackers stealing user data from the platform, with the identity of the hackers remaining unknown to this day. The hackers appropriated data and subsequently sold it. The hackers compromised the platform's security and accessed all sensitive user information. These case studies provide insight into the expanse of cyberspace and underscore the necessity of raising awareness regarding the occurrence of such crimes, while also emphasising the imperative to investigate these offences by introducing innovative concepts and mandating the role of cyber police to take prompt action.

SUGGESTIONS

We are unable to address the challenges that are presented by cyber criminals, even though there are laws and international norms regarding this matter. Taking action to address these concerns is mandatory. I would like to make the following recommendations to improve the efficiency of cyber policing and counteract the problem of cybercrime.

- **Education**: The proliferation of technology has granted universal access to the internet and smartphones. For educational purposes, we have integrated technology into classrooms, and cyberspace is now utilised for financial, educational, and recreational activities. This serves as a reminder to educate all individuals about cyberspace. Instructing children and adults on the nature of cyberspace, as well as the laws and initiatives implemented to safeguard against cybercrimes. A mandatory curriculum should be implemented in educational institutions, and a mandatory training program should be implemented for professionals, to raise awareness about crimes of this nature and the importance of reporting them to the appropriate authorities.
- **Cyber Security Firms**: The government must collaborate with international cyber security firms, establish agreements such as Memoranda of Understanding, and grant them the autonomy to function as cyber law enforcement entities. Independent cybersecurity firms may receive pre-approval from governments, serving as the primary resource to assist law enforcement in fulfilling its responsibilities. Cybersecurity experts are essential, and such firms offer a reliable platform that the government can depend on. Granting this firm autonomy to operate within state regulations will enhance cybersecurity and improve the efficacy of cyber policing. Their role is critical, as evidenced by the "WannaCry Ransomware Attack," in which a cybersecurity expert from a cyber firm proved valuable in resolving the issue.
- **Role of International Law**: International law must be enforced within the realm of cyberspace. The international community must confront the challenges posed by cybercrime and cyber policing. It is my belief that an international treaty is necessary, requiring ratification by members of the international community and implementation within their domestic legislations. The implementation of this measure would ensure that all cybercrimes that take place in any jurisdiction are dealt with in a consistent and fair manner. In addition, there is a need for the establishment of an independent international cyber tribunal to address potential trans jurisdictional issues and ensure that justice is maintained among member nations. In this court, individuals who have been harmed by cyber-crimes or crimes that have affected the country could file an independent case. Through this court, cyber experts can conduct comprehensive investigations and hold the perpetrators accountable for their actions. International law can play a pertinent role to bring about changes and the need is to create awareness and raise concerns for cyber security.
- **The necessity for victim support services**: Any cybercrime can adversely affect an individual's mental and emotional well-being. An immediate necessity exists to implement a victim support service mechanism for individuals affected by cybercrime. These centres can assist victims in overcoming emotional trauma and facilitate their reintegration while educating them about cybersecurity. These centres can be a driving force to help individuals going through emotional hardships faced due to cyber-crimes.
- **Cyber Police**: It is essential to recognise the necessity of an autonomous cyber policing framework. The Hon'ble Supreme Court of India has emphasised the necessity for an independent cyber policing unit that functions autonomously from the regular police force. To

differentiate between digital police and investigating officers and other law enforcement personnel, a distinction needs to be established. While a trained team needs to be established, a legal framework that mandates the formation of such a team would help reduce the number of cybercrimes and ensure that those responsible are held accountable.

CONCLUSION

There has been an increase in cybercrime because of the introduction of technology into everyday life and the digital realm. It is imperative that laws be put into effect and that awareness be raised at this very moment. If we are aware of the rights that we possess, how we can report crimes of this nature, and the measures that will be taken, then the fear of the people would reduce, if anyone committed such a crime. This is because they would have faith in the cyber policing mechanism and in the laws that are designed to punish those who commit such crimes. The digital space will present such challenges, and cybercriminals will take advantage of them. However, as individuals, we have a responsibility to keep ourselves informed about the initiatives taken by the government, to suggest that the government act, to file public interest litigations, and to seek justice and corrective measures from the court to reduce the number of crimes of this nature and to hold those responsible for offences of this nature accountable. In this context, the identification of data through cyber police becomes more important to check what crimes are being committed, as well as the number of crimes of this kind that are being committed using the same IP address, and to locate those responsible. Even though India has robust legislation in place to ensure that cyber criminals are held accountable for their actions, we still need to ensure that these laws are enforced and that we create an environment in which everyone is aware of their rights and cyber security.

*****

SHIFTING REALITIES: ADDRESSING THE LEGAL AND ETHICAL CHALLENGES OF DEEP FAKES IN INDIAN JURISPRUDENCE

Shubhangi Pandey[23]

ABSTRACT

Artificial intelligence and machine learning have given birth to a very significant evil of the digital world known as Deepfakes. It is a form of manipulated media that allows for the creation of fake and fabricated videos, photos, and audios. Two major forms of deepfakes that are common in society are political and pornographic fakes. Political deepfakes defame the political leaders, which can lead to manipulation of the electoral results in the post-truth era, while pornographic deepfakes often consist of face-swapping, wherein a person's face is superimposed onto another body, creating the delusion of sexual activity. With the increase in the advent of penetration of social media, there is a growing potential for deepfakes to intrude into various professional and personal domains. It threatens the privacy and security concerns of the masses, including the celebrity figures of different domains. Deepfakes have also disproportionately affected women, particularly in the form of non-consensual pornography and harassment. The political dispensation across the globe is endeavouring to take action against it, with the likes of India banning TikTok while the U.S. exploring the privacy concerns of the aforesaid platform. Current Indian laws like the Information Technology Act, 2000, and Bhartiya Nyaya Sanhita, 2023, fail to address the rising deepfake issues imbibed in the country. This paper throws light on the need for a regulatory framework to protect infringement of privacy and manipulation of public opinion at large. This paper further explores legislative reforms and highlights the importance of raising public awareness and ethical measures to mitigate the risks posed by deepfakes. Through a targeted series of legislative and consultative approaches to promote digital awareness, India can work toward creating a safer digital environment.

Keywords: Deepfakes, privacy violations, Information Technology Act, 2000, Bhartiya Nyaya Sanhita, 2003, Legislative Reforms

INTRODUCTION

AI and machine learning have benefitted our society in several manners, including a wide spectrum of industries, namely entertainment, business, and healthcare. However, on the flip side, these artificial technologies have also paved the way for darker applications, including deep fakes. Deep fakes are created through artificial intelligence that in turn manipulates or fabricates images, videos, audios, etc. The main aim of the technology is to recreate gestures, voice, and face to make it seem real.

If we talk about the entertainment industry, this deep fake technology improves the effects through aiding and language dubbing for movies. It is utilised primarily to curb public opinion, cyber harassment, and violate the privacy of an individual. Major deep fakes are happening in politics and pornography, where they are exploited to defame political leaders or generate non-consensual explicit content. The penetration of social media with its current state of being less regulated has provided a breeding ground for deepfakes. It poses a threat to the security and privacy of every individual, including politicians, celebrities, etc. This paper throws light on the ethical, legal, and regulatory

[23] Assistant Professor at SAGE University, Indore, India.

challenges associated with the current legislation governing this evil impliedly, namely, the Information Technology Act, 2000, Bhartiya Nyaya Sanhita, 2023, the Copyright Act, 1957 etc.

The current situation is knocking doors for ethical guidelines, public awareness, and legislative reforms to combat the potential risks of deepfakes. The world has witnessed the infamous video of Donald Trump being insulted by Barack Obama, which resulted in the spread of misinformation quickly and rapidly into the public domain. Unfortunately, this evil has yet to garner the legal attention as required, in spite of the fact that the cases related to revenge porn and political manipulation have transcended mainstream society.

TYPES OF DEEP FAKES

- **Political Deepfakes and Manipulation of Public Opinion**

It is one of the significant tools used by individuals to malign the image of political opponents and manipulate election mandates. This technology is used to create realistic videos of politicians with false or damaging statements. This leads to profound influence upon voters, including social unrest and influencing voters.

The infamous deep fake video of Barack Obama was debunked eventually; however, its circulation highlighted the ease of spreading misinformation. This particularly alters the pathway of geopolitical events and political campaigns. The emotionally motivated storylines have displacing the authentic and manipulated content in the post-truth era, and it is quite difficult to distinguish between the truth and false narratives.

The institutions of democracy have been severely compromised with the diminishing trust in public figures and rapid spread of misinformation. Even the voter perceptions are getting affected by the deepened political polarisation and interference into the functioning of democracy. In comparatively young democracies, the political deepfakes lead to strong social and ethnic disharmony leading to the civil war and toppling of the government, while in the case of mature democracies, it is used to violate freedom of speech and expression, thereby suppressing the dissent of the common people. Chesney and Citron (2019) have long been termed Deepfakes as weapons of mass deception and can have a significant impact on global security, particularly during election cycles and periods of political unrest.

- **Pornographic deepfakes and gender-based harassment**

The non-consensual pornographic content is a major concern, and misuse of deepfake technology, which primarily targets women, It is usually done through the superimposition of a person's face into explicit sexual content without the knowledge or consent of the victim of deepfake. This leads to tarnishing of image, defamation, and misuse of copyright and personality rights associated with the victim, and the impossibility to control the widespread use of content uploaded online turns into a misery and tragic scenario for the same.

Often, celebrity women are being targeted through pornographic deepfakes. One of the incidents in the past involved actress Scarlett Johnson, wherein she expressed her helplessness to combat the ongoing generation of fake explicit videos related to her image and video. Adult content websites are filled with

the generation of such deep fakes and thereby lead to widespread abuse, contrary to their public opinion of being a niche tool.

Non-consensual porn not only leads to violation of the privacy and dignity of the victim but also facilitates a pathway of cyber harassment of the victim. Law authorities and victims face a major challenge in removing the content, often across international boundaries, as it makes it hard to identify the perpetrators. In the case of ordinary women, the situation becomes worse as they even lack the resources to choose the legal recourse.

In research done by Studies by Stroud, AI-generated pornography has been considered the primary source of objectification of women, thereby making it a major source of digital sexual violence. Women are often left with no legal recourse and adequate protection to address these deepfakes.

PUBLIC TRUST AND MEDIA INTEGRITY

One of the most common concerns of the deepfake technology is that it takes away public trust and establishes a sense of prejudice in the minds of the viewers. In this digital age, individuals are dependent largely upon the visual and auditory cues to assess the authenticity of the content. It also disrupts the credibility of media institutions.

The conventional way of journalism through relying upon video footage, audio, and witness testimonies has been compromised severely. It no longer guarantees the authenticity of the content, and it seems very difficult to do credible reporting by the media institutions. The risk of information nihilism emerges with the advancement of AI-generated content, wherein individuals discard the authenticity of any media content irrespective of its legitimacy. Rini (2020) terms this phenomenon an 'epidemic backstop,' which means our potential inability to form a shared understanding of inability that is imminent to democratic processes and electoral reforms.

Digital media has further increased the vulnerability of deepfakes as people are more glued to sensational, inflammatory, and shocking content. These leave an indelible stigma on public perception and misinformation.

DEEPFAKES THROUGH LEGAL LENS

The legal framework in India is not sufficient enough to combat the penetration of deepfakes prevalent in our digital network. The legislation lacks explicit provisions to cover the wide ambit of deepfakes, as there is no evident legal provision to combat AI-generated content relevant to the industry.

- **Information Technology Act, 2000**

Various provisions of the Information Technology Act, 2000, including Section 67A, cover some aspects of deepfake-related content, which criminalises the distribution of obscene material. Similarly, Section 66E of the Act talks about the privacy of an individual violated by the unauthorised recording, publication, or transmission of an individual's images in mass media using deepfake technology.

On the aforesaid lines, an individual who maliciously deceives or impersonates someone through communication devices or computer resources is combated by Section 66 D. The penalty and

imprisonment provisions are imposed upon the said violation. However, its outdated language takes away the penetration to cover the intricacies of deep fakes within its ambit.

- **Information Technology Rules 2021**

The Ministry of Electronics and Information Technology has released advisories to social media intermediaries to combat deep fakes. One of the advisories dated 7th Nov 2023 released by the aforementioned ministry to identify misinformation and deep fake comprised suggestions pertaining to devising protocols to not allow posting anything that is forbidden by Rule 3(1)(b) of the IT Rules. In case of any violation, there will be legal repercussions. Any content that is prohibited by the IT Rules needs to be made apparent to users.

Another advisory dated 26th December 2023 was released by MeitY to comply with existing IT Rules, which dealt with reasonable efforts that needed to be identifying misinformation and deep fakes. It also focused upon due diligence by social media intermediaries that violate user agreements, rules and regulations, and other relevant guidelines.

The said advisory prompted users to refrain from hosting more misinformation, content, or deep fakes. It also urged the platform to remove any content that is reported within 36 hours of the incident, and access to the content that is in violation of IT Rules 2021 needs to be disabled.

These advisories make it evident that the casual approach from the platforms and intermediaries could result in them being blocked. The platform under Rule 3(1)(b) of the IT Rules 2021 is supposed to comply with the guidelines pertaining to the obligations of the same.

- **Indian Penal Code, 1860**

The Indian Penal Code (applicable before Bhartiya Nyaya Sanhita, 2023) used to contain provisions like forgery (section 465), defamation (section 509), criminal defamation (section 499), and spreading hate on communal lines (section 153) that may be invoked for cybercrimes, including the offence of Deepfakes. However, the language and intention of these sections could not anticipate the evils of Deepfakes.

- **Copyright Act, 1957**

The Copyright Act, 1957, is comprehensive legislation relating to the protection of intellectual property rights of an individual. Deepfakes not only leads to cyber harassment but also violates the copyright of an individual associated with such content. It uses photos, videos, audios, etc. of a person to impose it upon some other content without the consent of the individual. Section 51 of the Act impliedly deals with such incidents as it comprises various offences, including copyright infringement. It tries to provide protection to the original work of the content, including music, films, and creative content.

- **Personality Rights**

Personality rights are associated with mostly celebrities or well-known individuals relating to certain acts or a gesture that makes them synonymous. In the recent past, actor Anil Kapoor obtained a protection order from Delhi High Court pertaining to the misuse of his name, likeness, voice, and

distinctive features from being misused by Deep Fake's technology. Similarly, Amitabh Bachchan was granted similar protection when his public image was used without his consent, resultant to the dangers posed by deepfake technology and the necessity of protecting people from its misuse.

However, there is an evident need to put a stop to the propagation of false and fabricated information about public figures and misinformation around them. The legislators need to find balance between the fundamental and intellectual property rights and legislation to curb deep fake technology.

LEGAL CHALLENGES RELATED TO DEEP FAKES

The widespread outrage of deep fake technology has outpaced legal frameworks around the globe, including India, and has posed some significant challenges pertaining to it. The legislation has been enacted to curb things done by humans largely through conventional methods.

- **Defamation and privacy violations**

This is one of the most significant legal challenges posed by deep fakes. It particularly maligns the image of the victim in the eyes of common people and leads to reputational damage. Section 499 of the erstwhile penal code comprises defamation, while Section 500 of the code deals with the punishment up to two years. In addition to that, the privacy standards as recognised by the Hon'ble Supreme Court in Justice K.S. Puttaswamy v. Union of India under Article 21 of the Constitution are getting violated by the deep fakes, as it does not particularly misuse images and videos used through this technology.

- **Manipulation of Evidence**

It poses audiovisual evidence as the fakes lead to fabricate evidence, wrongful accusations, or acquittals. Further, it jeopardises the forensic tools and is capable of detecting deep fake content. It is the inability to manipulate video footage or audio recordings that makes it difficult to test the authenticity of such evidence in court.

- **Forgery and Fraud**

Section 468 of the IPC, along with Section 66 D of the IT Act, 2000, fails to address the forgery and fraud done with the complexities of deep fakes that involve sophisticated AI techniques and are not easily detectable by the intention of the language used in the provision.

- **Consumer Protection and Data Privacy**

The deep fakes are even affected by the terms and conditions of the Zao app, as it allows perpetual rights over users's images. These images may be potentially damaging the privacy of consumers of the applications.

INTERNATIONAL LEGAL APPROACHES

There are various approaches taken by different countries in order to combat deep fakes and manipulation that should be witnessed closely in order to witness its effectiveness.

- **United States**

The United States has adopted the law against deep fakes both at the federal and state levels, such as California's AB 730 law, which takes care of the prevention of deep fakes within 60 days of an election to deceive voters. It seems to be one of the significant approaches to lessen the penetration of manipulation during the election time through AI-generated content.

Even the Deepfake Report Act of 2019 highlighted the issue of national security and privacy concerns in the U.S. However, these laws have not stood the test of time, as they are at the nascent stage of evolving to keep pace with rapidly advancing technology.

- **European Union**

In the European Union, the GDPR provides various remedies for victims of deep fakes. It provides the users with the right to request the removal of content that infringes on their privacy. However, the fakes are created anonymously or hosted on servers outside the EU, and the enforcement of such requests always remains a challenge.

- **China**

At the onset of the pandemic, China has come up with a stringent regulatory approach in 2020 pertaining to deep fakes. It puts misinformation under the check through the Cyberspace Administration of China's implemented rules requiring AI-generated content. Their approach and understanding of the regulation is a comparatively stricter way to address the issue, as it also points concerns about freedom of expression and state censorship.

ETHICAL CHALLENGES OF DEEP FAKES

Other than legal challenges, there are numerous ethical challenges related to deep fakes that have an immense effect on internet users. Deep fakes deal with various intricacies, including truth, consent, and privacy, which form the basis of this ethical dilemma. It gives us the moral compass to devise the development of AI and its use.

- **Consent and Autonomy**

It is one of the important ethical challenges that is considered mainstream in most of the deep fake incidents. Like in the case of deep fake pornography, there is an evident absence of consent and an undeniable harm. Even an individual's consent to the use of their likeness in one context can be misused in another context using deep fake technology.

The lack of consent of the victim in most of the deep fake incidents violates the principle of autonomy, wherein the image and likeness of the victim are used. It raises ethical concerns about the right to monetising deep fake content, distribution, and creation.

In the context of political figures, there is a debate around the ethical question of whether the public's right to satire or political commentary should outweigh an individual's right to control how their image is portrayed.

- **Privacy Violations**

Privacy is one of the other ethical challenges that are faced by the deep fakes. The major concern regarding the deep fakes is that they use the personal images and videos shared by the individuals on social media platforms. Even the CCTV cameras and the availability of personal data on public platforms make individuals vulnerable to such deep fakes violating the privacy norms. The laws related to privacy deal with the protection of traditional ways of privacy. However, it falls short when the realistic images or videos of individuals without their knowledge blur the boundaries of privacy.

- **Harm Principle and Responsibility**

Deep fakes pose a serious threat to the harm principle, according to which the individuals and organisations are supposed to not cause significant harm to them. It leads to emotional distress through activities like pornographic deepfakes or political misinformation, and the potential for harm is evident.

Social media intermediaries like Facebook, Twitter, or YouTube even struggle to combat the ethical challenge of the harm principle as the volume of content makes it difficult to effectively police. Another important concern is to address the responsibility of such deep fakes between the individual who creates such deep fakes or such platform that hosts the same.

- **Manipulation and Deception**

This is another ethical challenge for deep fakes, as it manipulates not only individual perceptions but also collective beliefs. The deceiving nature of deep fakes, as it will become difficult for individuals to identify between reality and fake. It leads to the inability to make informed decisions based on reliable information.

- **Impact on Free Speech**

Deep fakes pose a threat to a balance between the freedom of speech and expression and harm caused to individuals, as often deep fakes are used for satirical and political commentary. One potential way to address this problem is to adopt a graded approach wherein different types of deep fakes are subject to different levels of scrutiny.

WAY FORWARD & CONCLUSION

The deep fake phenomenon is critical to the legal, ethical, and regulatory frameworks of the digital content. It possesses required potential that can take away with public trust bestowed upon them. Further, it leads to violations of privacy and cyber harassment. The specific legislation in India is supposed to match the pace with the immense development of AI technology. The age-old legislation needs to be revamped with the inclusion of the mandate of the AI.

On the same note, a singular set of legal responses would not be able to cater to the issue of deep fake. Even ethical guidelines need to be updated accordingly to promote the public good and individual rights. In addition to it, certain technological solutions need to be explored that can immediately block out the unauthorised use of images and videos through blockchain-based verification.

At the end, an integrated approach is necessary to combat the impact of deepfakes through working with various agencies of governments, tech companies, and civil society so that a secure and safer digital environment can be ensured in a digital era. Thus, adoption of a combination of solutions would help

in addressing the risks posed by deep fakes so that AI in the true sense can assist the human kind and not harm the same.

*****

BIBLIOGRAPHY

1. The Constitution of India, 1950
2. Information Technology Act, 2000
3. Bhartiya Nyaya Sanhita, 2023
4. Copyright Act, 1957
5. What is deepfake technology? https://www.techslang.com/what-is-deepfake-technology/
6. Raina Davis, Chris Wiggins, Joan Donovan, Deepfakes, SPRING 2020 SERIES, Rev, 1, (2020) https://www.belfercenter.org/sites/default/files/files/publication/Deepfakes_2.pdf
7. JM Porup, How and why deepfake videos work — and what is at risk, CSO INDIA , https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html
8. Westerlund, Mika. The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review. 9.. https://www.researchgate.net/publication/337644519_The_Emergence_of_Deepfake_ Technology_A_Review
9. Francis Navarro, Deepfake porn videos are now being used to publicly harass ordinary people, KIM KOMANDO.COM, https://www.komando.com/security-privacy/deepfake-pornvideos-are-now-being-used-to-publicly-harass-ordinary-people/526877/
10. Clare McGlynn, Erika Rackley & Ruth Houghton, Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse, Fem Leg Stud 25. Rev.25, 46 (2017). https://doi.org/10.1007/s10691-017-9343-2
11. Stroud, Clare. "AI-Generated Pornography and the Objectification of Women: A Feminist Perspective." Journal of Gender Studies, vol. 27, no. 3, 2018,
12. Press Infomation Bureau, MeitY issues advisory to all intermediaries to comply with existing IT rules,
13. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1990542&ref=static.internetfreedom.in
14. Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445
15. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code). Rules, 2021
16. Rashmi Senthilkumar, Defamation law in India, LEGALSERVICEINDIA.COM http://www.legalserviceindia.com/legal/article-2224-defamation-law-in-india.html

17. Parth Tyagi and Achyutam Bhatnagar, Deepfakes and the Indian legal landscape, INFORM.ORG, https://inforrm.org/2020/07/03/deepfakes-and-the-indian-legal-landscape-parth-tyagi-and-achyutambhatnagar/
18. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
19. Anil Kapoor vs Simply Life India & Ors CS(COMM) 652/2023
20. Grace Shao and Evelyn Chen, The Chinese face-swapping app that went viral is taking the danger of 'deepfake' to the masses, CNBC, https://www.cnbc.com/2019/09/04/chinese-faceswapping-app-zao-takes-dangers-of-deepfake-to-the-masses.html
21. Nilesh Christopher, We've Just Seen the First Use of Deepfakes in an Indian Election Campaign, VICE.COM https://www.vice.com/en_in/article/jgedjb/the-first-use-of-deepfake s-in-indian-election-by-bjp
22. Human rights in the age of Artificial Intelligence, https://www.accessnow.org/cms/asse ts/uploads/2018/11 /AI-and-Human-Rights.pdf.

*****

ADDRESSING ONLINE GENDER-BASED VIOLENCE: LEGAL LIMITATIONS AND HUMAN RIGHTS CONCERNS IN CYBER SPACES

Ruthuparna M.N.[24] and Yeshas B.S[25]

ABSTRACT

Online Gender-Based Violence (OGBV) is one of the emerging forms of abuse in the face of rapid growth of digital spaces and social media platforms. This research paper points out several dimensions of OGBV to understand how such violation impacts certain core human rights, namely privacy, freedom of expression, and equality. The main aim of the paper would be to hit disproportionately women and marginalized gender identities with key forms of abuse, such as cyberstalking, doxing, revenge porn, and online harassment. In doing so, it will discuss how such platforms contribute to the unfriendliness of these groups through weak regulatory mechanisms and content moderation policies. This paper will consider some of the most well-known cases of OGBV that have come to light in India: the notorious Bois Locker Room scandal, but also the Sulli Deals and Bullibai app cases, although the latter kind of two are not as sensational or recognizable: the diffuse, widespread online harassment of female public figures and journalists. This paper thus analyzes these cases to condemn the current legal structures of the Indian State, i.e., the Information Technology Act of 2000 and relevant provisions of the Indian Penal Code (IPC) and the new Bharatiya Nyaya Sanhita (BNS), as an ineffectual legal structure for effectively protecting OGBV. The paper highlights challenges in enforcing the aforementioned laws, and the lack of proper support systems to a victim of such crimes. Hence, in addition to calling for greater accountability on the platforms, more stringent laws, and policies tailored for the victims, their fulfilment calls for that they are achieved now in both their legal and psychosocial capacities. This requires a study of the existing international human rights frameworks such as CEDAW or the Convention on the Elimination of All Forms of Discrimination Against Women. This paper would look to develop a comprehensive strategy for addressing OGBV: legislative reform, digital literacy programs, and global cooperation toward safer online spaces for all genders.

Keywords: Online Gender-Based Violence (OGBV), Cyber Harassment, Human Rights, Privacy Violations, Platform Accountability.

INTRODUCTION

The internet and the social media revolution represent a new age of worldwide interaction and communication that brings utterly new changes to the ways in which people communicate with one another, the way they share information and participate in public debate. This digital revolution has unparalleled opportunities in connection, education, and empowerment but also new forms of abuse and harassment, Online Gender-Based Violence, OGBV, has indeed presented itself as a major challenge in the digital age, according to Gordon.

OGBV refers to any gender-based violence committed, assisted or aggravated using information and communication technology against a person on the ground that their gender is. This kind of violence affects disproportionately women and other marginalized gender identities. Such violence encompasses a spectrum of abusive behaviours that include cyberstalking, doxing, revenge porn, and online harassment.

[24] Student at K.L.E Society's Law College, Bangalore, India.
[25] Student at K.L.E Society's Law College, Bangalore, India.

Beyond the digital world, the effects of OGBV continue with violations of glaring basic rights of privacy, freedom of speech, and equality. Victims of OGBV face extreme psychological distress with social exclusion, and even danger, sometimes in the real world where online threats translate into actual violence. The insidious and public nature of the abuse, which is incessant, might have long-term impacts on personal and professional lives for victims, limiting their participation in digital spaces as well as reinforcing gender inequalities in broader society.

The anonymity and borderlessness of the internet made the fight against OGBV very challenging. Deep-rooted legal systems, which are mainly comprised of structures of accountability designed to handle situations outside the internet, are already brought to their limits as they strain to keep pace with these ever-changing statuses surrounding abuse on the internet. This mismatch between law and its application has developed an environment where perpetrators of OGBV can almost go about with impunity, and victims have very little avenue for justice or protection.

In the recent past, problems of OGBV have emerge as some of the most widely commented-upon concerns in India, as high-profile cases in the media present the gravity and prevalence of the problem. From the "Bois Locker Room" scandal showing pictures of underage girls shared by schoolboys to the "Sulli Deals" and "Bulli Bai" apps that "auctioned" Muslim women online, such incidents have garnered national outrage and necessitate sterner countermeasures at law and in society against OGBV.

In the context of such laws as the Information Technology Act, 2000, and relevant sections of the Indian Penal Code, these legal instruments leave an incomplete impact in the prevention of OGBV. Jurisdictional issues plague cybercrime cases, and technical grounds go hand in hand with a lack of specific provisions to deal with the unique aspects of online gender-based violence.

This paper will look into, from a research point of view, the nature and the scope of OGBV in India, evaluate effectiveness of legal measures available so far, and suggest comprehensive methods to combat this issue which is really developing. In this research, there will also be an exploration of key case studies and considerations of national as well as international legal frameworks in relation to OGBV to bring about better approaches to handling OGBV.

The objectives of this research are:

1. The various modes in which OGBV occurs and its impact on human rights, specifically in relation to privacy and freedom of speech and equality.
2. Study the most notable cases in the context of OGBV in India, which includes the "Bois Locker Room," "Sulli Deals," and the app "Bulli Bai" to understand the patterns and effects of online harassment.
3. How effective are India's legal frameworks-including the Information Technology Act, 2000, Indian Penal Code, and the new Bharatiya Nyaya Sanhita (BNS)-in dealing with OGBV?
4. How effective are international human rights frameworks in dealing with OGBV? To critically study the same, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) has been focussed upon.

5. To propose a comprehensive, multi-pronged approach for addressing OGBV through legislative reform, accountability on the platforms, victim support systems, and global cooperation.

In order to address such goals, this paper will contribute to the already deeply debated OGBV issue, providing policymakers, legal professionals, and digital platforms with concrete steps on their way toward the objective. It is about reducing the potential violence and enhancing the online public safety by conducting a systematic assessment of the effects of OGBV on female victims' personal rights.

Thus, going into the specifics of OGBV, we realize that it is not just an issue that can be so easily dealt with but one at the intersection of technology, gender, and law. Therefore, tracing these conversations and challenges while proffering possible solutions geared at bridging that gap between the constantly shifting digital space and legal frameworks intended to protect people within it is what this paper will do.

UNDERSTANDING ONLINE GENDER-BASED VIOLENCE

Forms of OGBV

Online Gender-Based Violence refers to a broad range of abusive behaviours enabled by digital technologies. Common forms of OGBV include:

1. **Cyberstalking:** Repeated, unwanted online monitoring of a victim's activity often coupled with threats and psychological intimidation.
2. **Doxing:** Unauthorized release of private or personal information in social media, hence exposing victims to actual and psychological harm.
3. **Revenge Porn:** They are the intentional posting of intimate images with no consent mostly done to shame and control victims.
4. **Trolling and Online Harassment:** Gendered abuse, which includes death and rape threats, is used to muzzle women and marginalized genders on line.

These are the publicized harassments that are mostly faced on digital platforms, and hence the impact is more extended and not easy to be dealt with.

HUMAN RIGHTS CONSEQUENCES

The fundamental right of the victims is severely impacted due to the radical outcome of OGBV, as found below:

1. **Privacy Violations:** In OGBV, private information or content is oftentimes disclosed without consent, violating the right to privacy guaranteed by Article 21 of the Indian Constitution.
2. **Freedom of Expression:** Women, activists, and LGBTQ+ individuals are disproportionately more vulnerable on social media platforms to receiving violent threats; women become "silenced" and reduced their participation in public debates as a result.

3. **Equality:** OGBV mainly centers on excluded gender identities, hence propagating some flawed gender stereotypes, which are already forms of existing inequalities in the genders.

The United Nations Human Rights Council identifies online harassment as the significant barrier to women's full participation in society, compelling OGBV to be a global human rights concern.

OGBV IN INDIA: CASE STUDIES

India has witnessed a number of high-profile cases of OGBV that presents the depth of the issue and its result are drastic below:

1. Bois Locker Room Scandal

"Bois Locker Room" is a scandal that came out in May 2020, a private Instagram group chat involving schoolboys from Delhi, where images of underage girls were being circulated against their will and disgusting discussions on sexual violence were going on. It catalyzed national outrage and brought focus to the all-pervasive nature of women's and girls' online objectification and harassment.

The case exposed the void left by the present legal system in matters such as these, mainly when children are involved. It also stressed the need for good-quality digital literacy programs and tighter regulation of social media applications.

2. Sulli Deals and Bulli Bai Apps

In two successive but well-related incidents in the years 2021 and 2022, the apps named "Sulli Deals" and "Bulli Bai" were made to "auction" some Muslim women, activists, and journalists. The images of the ladies appeared without their consent on these apps and exposed them to communal as well as gender-based harassment.

These incidences are a representation of how OGBV cuts across intersecting axes where women belonging to the marginalized sections are discriminated based on gender and religion. While people were arrested in such cases, these incidents revealed deep structural failures in shielding vulnerable groups from strategic attacks.

3. Cyber Harassment of Women Journalists

In India, female journalists here are constantly targeted and harassed on the internet with concerning severity, especially those reporting sensitive topics or controversies. Some of the celebrated journalists, like Rana Ayyub, had to face misogynistic hate speech and threats of sexual violence plus doxing because they voice their critical opinions.

Such abuse curtails freedom of speech at the same time as threatening democratic participation; it suppresses the opposition voices. This case calls for strengthening legal protections and more effective mechanisms of enforcement in order to ensure freedom of expression in digital space for women journalists.

INDIAN LEGAL FRAMEWORKS

Information Technology Act, 2000

The main enacted law of the country relating to cybercrime, including Online Gender-Based Violence (OGBV) is the Information Technology (IT) Act, 2000. This enactment was made without any explicit thought on OGBV as an instrument against the same. It is read and constructed to address certain forms of digital violence. Notably by the way, the provisions of Section 66A dealt with sending "offensive messages" through communication services. The chapter, however, fell because it was drafted in obfuscatory terms and stood poised to be used to choke free speech-an eventuality of which this court had, in Shreya Singhal v. Union of India (2015) held to be unconstitutional.

The consequence of this is the crucial lacuna wherein no specific provisions have been made that criminalize cyber abuse. The other section is Section 67, which criminalizes the publication or transmits "obscene material" in electronic form. Whereas this chapter can be stretched to an extent to include types of OGBV-such as revenge porn or explicit material posted online-this is also not applicable to a large extent. Example Section 67 cannot be accommodated under contemporary acts of OGBV, such as doxing-publication of private information-or cyberstalking-online surveillance.

It is considered to be an archaic provision and is not regarded as adequate enough to consider the complexities of OGBV.

Indian Penal Code (IPC): Sections of the Indian Penal Code (IPC) may also be referred to as evidence to take action against the OGBV. For instance, section 354D provides for stalking with any means whatsoever that adopts digital or online in some manner.

Again, this is an important application in the trials of digital harassment cases, but the interpretation of this law is not uniform, and even victims in most cases face problems in the first place to get justice either because of the societal stigma often attached to rape victims or because the police are reluctant to dig into digital complaints. Sections The above sections are also generally used for internet complaints against abuse, more often the case concerning criminal defamation under Section 499 of the IPC and criminal intimidation under Section 503. Yet the same sections were primarily drawn up in consideration of an offence that has already occurred offline and give little indication of scope or nature of OGBV.

For example, most the incidences of violence and cyber stalking are anonymous or cross-border which make it complicated tracing the culprit, therefore, would complicate the process of doing justice to them also.

Protection of Women from Domestic Violence Act, 2005: Although focused mainly on physical and emotional violence in the domestic sphere, provisions of the PWDVA, 2005 was also invoked in the case of cyber harassment. Section 3, Act defines domestic violence: which not only reflects in the act of physical abuse but also the kind of emotional and verbal abuse that can extend to cover OGBV when the abuser knows the victim, such as revenge porn or cyberstalking by an ex-partner.

However, as if it had been drafted with the off-line cases of intimate partner violence, PWDVA is restricted to its use in OGBV only due to its inadequacy in ascertaining the anonymity of the criminal in most the cases of online crimes.

The Bharatiya Nyaya Sanhita (BNS) Act, 2023: It imposes numerous provisions that bear relevance to addressing OGBV. Though the act does not pay specific attention to OGBV, various provisions indirectly affect the subject by updating the legal framework of digital-related crimes such as abuse and violations of privacy.

BNS introduces the category of organized crime under Section 111 that includes cyber-related offenses. It can therefore be invoked in cases where OGBV is carried out with the help of organized efforts which include coordinated harassment or trafficking for illegal purposes such as sexual exploitation.

For the first time ever, some sections have been amended to make them gender-neutral; for instance, stalking and voyeurism, which were formerly gender-specific under the IPC, are now made gender-neutral in BNS. That is, men as well as women can be prosecuted under these sections; otherwise, this goes one step further towards justice in the digital medium where offenders relating to OGBV could be male or female.

Voyeurism and Harassment: Offenses associated with voyeurism-that is to say, observing or photographing someone in private without his or her consent-or stalking, which are forms of OGBV, have been retained and consolidated. Sentences for such acts are severe and can even now technically reach online behavior invading privacy thus potentially making revenge porn as well as cyberstalking easier to prosecute under Indian law.

Section 69 of the BNS criminalizes "deceitful promises," for example false promises to marry that are very often associated with cases of revenge porn or exploitation after intimate relationships. This will add another layer of protection towards victims of OGBV who are deceived in both digital and real life.

BNS has incorporated provisions against the spread of false information and other harmful digital content, which may well fall under OGBV. This can be used where false or libelous information finds its way to malign the reputations of women and other vulnerable groups.

INTERNATIONAL OBLIGATIONS AND COMMITMENTS

India is also a signatory to many international conventions and treaties that enforce an obligation to the state to ensure human rights, amongst them, the right not to experience violence based on gender. For example, CEDAW or Convention on the Elimination of All Forms of Discrimination Against Women, and resolutions of the UN Human Rights Council, both demands how deep legal frameworks must be to prevent OGBV according to UN Women, 2020. (add citation) India has attempted to fulfil this obligation but still the domestic law cannot address the underlying problems with OGBV, especially from cyberspace due to the reason that it has faced an enforcement problem due to anonymity and jurisdiction.

In a nutshell, although legal frameworks appear to be ready and available in the books of India on which avenues may be utilized in approaching the issue of OGBV, it is very apparent that there are gaps with

significant magnitudes. There also seems to be a need for missing specific legislation with regard to digital forms of gender-based violence and laws to enforce or hold the participating platforms accountable in the fight against OGBV. Only such adequate reforms combined with the adoption of such OGBV legislation will ensure better protection for today's victims of such practices.

Legal and enforcement challenges in combating online gender-based violence.

Despite some awareness about OGBV and several laws intended to prevent this tide, the one major challenge still remains to be that of effective enforcement in India. OGBV has been described as hostile actions deliberately directed at persons on account of their gender online; it has different implications for women and marginalized gender identities. Legal provisions, even though available, display variable skills in implementing these and multiple barriers prevent effective dispensation of justice in such cases.

JURISDICTIONAL ISSUES

The major hurdles in dealing with OGBV are their cyber nature usually making it a transnational issue as cases start to flow across borders. Internet anonymity enables perpetrators to perpetrate injurious conduct without the true identities or locations being known. It goes very difficult if the perpetrator is sitting in some other country to get them prosecuted under Indian law. Like every other country, India too faces jurisdiction issues in this regard. The Information Technology Act, 2000, among other enactments of India, also provides legal remedies against the domesticated crimes of the internet and cyber space. However, when crime crosses its borders and commits cross border offences, such enactments become ineffective. For example, if some person sitting abroad indulges in doxing, cyber stalking or revenge porn against some other person sitting in India, the Indian judiciary has very little jurisdiction over this latter person. This cross-border nature of digital crimes complicates investigations and enforcement.

Moreover, mutual legal assistance treaties between other nations are also generally slow procedures, bureaucratic processes that are now hampering timely justice. That process for seeking cooperation in another country is also quite lengthy and complicated, requiring extradition treaties in other countries is a significant hurdle toward bringing criminals to justice.

Such international cooperation of social media companies is indeed necessary but not readily available in these cases involving the proofs to be fetched from outside India in the form of IP addresses or server logs.

Platform Accountability

While social media platforms play a very important role in the perpetuation of OGBV, they rarely act promptly or adequately on complaints of online harassment. Obligations to remove offensive content have been imposed by Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, but their provisions are often only insufficient in terms of covering the extent and intensity that obtains with OGBV.

Criticisms to these platforms have been towards laxity in accountability about OGBV issues and the tardiness in complaint handling. Active abuse against women and marginalized gender identities

includes rape threats, death threats, and doxing, yet reports on such matters are oftentimes ignored, delayed, or not acted upon.

The absence of stiff liability for social media companies allows OGBV to operate through the digital interface.

There is often extremely low transparency regarding complaints, how many are solved, and the action taken. Platforms are not by law mandated to make any disclosures relating to the data over the number of reports received concerning OGBV; neither must they describe the action taken toward their efforts at protecting victims. Such a scenario prevents the public or regulatory bodies from holding these platforms accountable for their part in facilitating such behaviour.

Victim Support and Social Stigma:

There is also social stigma attached to an OGBV victim, which deters many victims from coming forward. Victims of online abuse in India are predominantly women exposed to victim-blaming attitudes. This creates an atmosphere that deters victims from approaching law courts out of fear of social ostracism and reputational damage.

This tragedy is altogether unwarranted since most victims of OGBV remain uninformed both about their rights and ways of redress. Without complete victim support structures, including legal assistance, counselling services, and rehabilitation programs, the tragedy is altogether unwarranted. Victims of OGBV usually suffer very serious psychological effects among them anxiety and depression and, in many cases, post-traumatic stress disorder. In the absence of sufficient mental health support, such people are left exposed to further abuse.

Also, the law enforcement agencies in India generally do not have facilities for digital complaints. The cyber cells of the police are still in a developing stage, and there is a scarcity of technical expertise regarding complex cases of OGBV. The insensitive nature of the police personnel towards the type of OGBV is also one of the reasons, as they treat OGBV as less heinous than any other physical crimes, and victims are deterred from reporting such incidents.

Moreover, the slow process of judicial prosecution in India discourages many victims from pursuing justice.

ADDRESSING OGBV: PROPOSED SOLUTIONS

To combat OGBV, an approach is multifaceted given the challenges seen in its relation. Included are legal reforms, platform accountability, victim-centric policies, and international cooperation that must aim to attack the problem comprehensively.

Legal Reforms

The specific legislation dealing with forms of digital violence has to form one of the first steps in addressing OGBV. No specific law deals with OGBV in India. Such a gap pushes victims to rely on vague and outdated provisions that were never designed to deal with the digital world. Definition, criminalization, and penal provisions in specific laws are required for OGBV behaviours in the form of cyberstalking, doxing, and revenge porn.

1. OGBV Legislation: India needs to have special legislation which specifically caters to OGBV. This legislation may include the legal definition of various types of OGBV and rigid penal provisions for offenders. There should also be a specific clause that deals with cross-border jurisdiction and presents mechanisms for international cooperation in order to prosecute cases of OGBV.
2. Reformulation of Existing Laws: Already prevailing laws, like the IT Act, 2000, and the Indian Penal Code (IPC), must be reformed so that their digital nature would qualify for OGBV. The IT Act must specifically include laws that criminalize doxing, revenge porn, and cyber harassment. The IPC likewise needs reformulation in light of the kind of offensive faced while dealing with anonymous perpetrators.
3. Expedited Legal Processes: Special courts or fast-track procedures should be established for OGBV cases to ensure timely justice. Victims of OGBV often face lengthy legal battles, during which they continue to experience abuse and harassment. Expediting the legal process will provide relief to victims and serve as a deterrent for future perpetrators.

Platform Responsibility

Hold social media platforms accountable for their role in fuelling the spread of OGBV. Also, more stringent regulations must be enforced to ensure active moderation and responsible tooling to fend off abuse to users.

1. Forced Content Moderation: To ensure that the platform adopts proactive content moderation measures and its implementation of highly advanced technologies, such as AI-based tools, for the identification and removal of abusive content, the law must make known such measures and hold it to ensure any offending content violating community guidelines was removed promptly.
2. Transparency Reports: Media should be mandated to make annual transparency reports showing the OGBV complaints received, the measure taken, and the time taken within the specified timelines to address complaints. This will also act as a check on platforms' accountability to the regulatory body and the population.
3. User Verification: More rigid verification processes for users are imperative to lower unauthorized use without affecting the issue of anonymity. Though there are areas where anonymity is needed, such as by people in activism or whistleblowers, it means that perpetrators of OGBV can operate freely because they have anonymity. A verification system could help find a balance between some issues of privacy and accountability.
4. Cooperation with the Police: Social media companies should have explicit policies regarding cooperation with law enforcement agencies. This cooperation will ensure swift inquiries and take-downs of violative content as well as the identification of perpetrators of OGBV.

Victim-Centric Policies

Effective responses towards countering OGBV must be centered on the victim's needs. Support struc-

tures must be developed for victims to provide them with justice and to recover from such experiences.

1. Legal Aid: There must be specific legal aid services to help OGBV victims receive justice in the court of law. These services would inform the abuse victims on how to file such cases, take legal action against the abuser, and receive compensation.
2. Counselling Services: The victims of OGBV are basically exposed to grave psychosocial challenges. Counselling services ought to be provided towards the victims from all potential sources, free or at a reasonable cost in order to help grapple through this traumatic situation caused by online abuse.
3. Digital Literacy Programs: Widespread digital literacy programs are essential for educating internet users about aspects of online safety, privacy settings, and how to report OGBV. These programs can empower the individual to further protect him or herself online and significantly reduce the rates of occurrence of OGBV.
4. Public Awareness Campaigns: The country should implement nationwide campaigns that will increase awareness of the existence of OGBV and dispel its social stigma. These campaigns should try to liberate victims from their fear of reporting due to victim-blaming or being judged.

International Cooperation

Because of the international character of the internet, combating OGBV demands cooperation among nations.

1. Cross-Border Legal Frameworks: There should be agreement, for example on cross-border jurisdictions, so that it becomes effective and safe to come together to address some of the challenges in OGBV cases.
2. Global Standards: India should be collaborating with international organizations to arrive at global standards in dealing with OGBV. These standards may then become included in a package of best practices from multiple countries and adapted for India. unique legal framework.
3. Knowledge Sharing: Create avenues for knowledge sharing among countries that would provide a channel for information, research, and strategy dissemination in the battle against OGBV. Such cross-national interaction may also strengthen each nation's capabilities to counter online abuse.
4. Harmonisation of Laws: There should be a harmonisation of cyber laws among countries with an eye towards similar protection of all victims in every country across the globe. The uniform legal approach will allow for the ability to combat cross-border abuse and an ability to hold abusers accountable wherever they may be.

CONCLUSION

In this regard, online gender-based violence is an issue that has become pervasive in this digital age, threatening fundamental rights, including those of women and other underprivileged gender identities.

Legal frameworks are in place to address OGBV, but they are usually inadequate and archaic, making the victims susceptible to continuous abuse. OGBV must be addressed as a complex and all-rounded phenomenon that needs legal reforms, platform accountability, victim-centric policies, and international cooperation. The strengthening of legal provisions on OGBV in addition to building responsiveness of the platforms also call for national and international stakeholders to collaborate in creating a safer and more inclusive space on the internet. Such will be the case with legal frameworks, with further developments in the world of the digital habitat. These will have to undergo a shift to meet the challenges developed by OGBV. Only collectively, through national and international efforts, is it possible to perhaps mitigate online abuse and ensure that all digital platforms are tools for empowerment, not instruments of oppression.

*****

NAVIGATING REVENGE PORN: SOCIAL MEDIA'S DOUBLE- EDGED SWORD

Dr. Chayanika Basu[26]

ABSTRACT

The examination of vengeance within a romantic framework has increasingly garnered attention in the social sciences. The exploration of factors influencing romantic vengeance is fascinating; yet, most studies have not delineated the specific types of romantic revenge people perpetrate and have overlooked the role of technology in the execution of such retribution. The emergence of social media has significantly altered communication and human connections, while also fostering troubling issues such as revenge porn. Revenge porn, defined as the non-consensual distribution of personal photographs or films, is increasingly enabled by social media platforms owing to its user-friendliness, anonymity, and swift dissemination capabilities. Perpetrators use the vast reach of social media to publicly disgrace, extort, or seek vengeance on victims, resulting in significant emotional, psychological, and even bodily damage. These platforms, characterized by their extensive worldwide user base and viral tendencies, serve as conducive environments for the extensive dissemination of harmful information. Nonetheless, social media significantly contributes to the avoidance and alleviation of revenge porn. Platforms have begun the implementation of more stringent content moderation standards, using artificial intelligence and machine learning to identify and eliminate non-consensual explicit material. Educational initiatives implemented on these platforms enhance understanding of digital consent, privacy rights, and the legal consequences of disseminating personal material without authorization. Moreover, social media offers victims access to support networks, advocacy organizations, and legal resources, enabling them to pursue action against perpetrators and get justice. Notwithstanding these gains, difficulties persist. The unbounded characteristic of social media complicates regulation, resulting in frequent deficiencies in platform responsibility. Thus, a collaborative initiative among social media corporations, law enforcement agencies, and lawmakers is crucial to formulate more effective preventative tactics and legal safeguards to prevent this menace.

Keywords: Romantic Revenge, Non-Consensual Distribution, Psychological Damage, Legal Safeguards, Support Networks

INTRODUCTION

Social media has transformed communication, information sharing, and public conversation. These platforms have promoted virtual communities and connection, but they have also enabled digital crimes like revenge porn. Retribution following romantic relationships is called "revenge porn" when explicit content is distributed without consent. Due to its virality, anonymity, and global accessibility, social media spreads such material quickly. Facebook, Instagram, and Twitter enable users to produce and share multimedia content without control, making them vulnerable to digital abuse. Many perpetrators use these sites' anonymity to escape identification and accountability. Perpetrators may hide their identities due to lax verification and bogus accounts, making justice harder for victims.

Social media spreads revenge porn, but it may also stop it. Social media companies' responsibility to prevent digital misuse and protect users' privacy is becoming more apparent. Platforms have taken technological and regulatory measures to stop revenge porn. A major technological intervention is using AI and machine learning algorithms to detect and prevent unwanted sexual information uploads.

[26] Assistant Professor at Balaji School of Law, Sri Balaji University Pune, India.

Facebook's "PhotoDNA" technology can digitally fingerprint revenge porn photos to prevent re-uploading prohibited content. Additionally, victims may complain and request removal of such content on social media. The creation of specialist teams to prevent non-consensual image transmission and clear reporting standards are improving response times and victim protection. Legal and regulatory initiatives by governments and social media platforms are combating revenge porn with technology advances.

THE ORIGIN AND GROWTH OF REVENGE PORN

In the early 2010s, revenge porn became a global issue, notably in Western countries like the US and UK. Increased access to social media and mobile phones led to the private sharing of personal content. As relationships fell, angry partners, mainly men, published or threatened to disclose this information online for retribution or extortion. Cultural, technological, and legal factors have fuelled revenge porn in India. Over the last 20 years, affordable mobile phones and internet access have transformed India's technology. This has transformed social interactions, increasing digital intimacy and abuse potential. Despite India's technological advances, patriarchal values prevail. Women are especially vulnerable to exploitation via the illegal dissemination of private material due to honour and shame connected with feminine sexuality. Revenge porn victims in India may face ostracism, victim-blaming, and violence. Sexuality taboos, particularly for women, worsen victims' experiences.

A female law student saw her personal photos and videos on social media in 2015 after her ex-boyfriend released them in retaliation. The case raised awareness of cybercrimes against women and legal gaps. Pornhub and other adult websites have also been criticized for posting revenge porn from India without proper removal or remedy. This exacerbates the problem since victims face social shame and a worldwide audience for their personal problems.

CAUSES AND IMPACT OF REVENGE PORN

The factors Contributing to the Proliferation of Revenge Porn on Social Media are as follows-

- A major factor contributing to the spread of revenge porn on social media is the supposed anonymity afforded by these sites. Individuals who disseminate non-consensual information often see themselves as insulated from legal and societal repercussions.
- The fundamental purpose of social media- information sharing- also facilitates the dissemination of revenge porn. Intimate photographs may be posted and disseminated over networks within seconds, becoming viral and reaching thousands of users before any measures can be implemented to delete the information. The simplicity of resharing and reposting exacerbates this issue, making it almost hard for victims to manage or withdraw their photographs once disseminated.
- Social media sites, whatever their efforts, often exhibit insufficient mechanisms for filtering and deterring revenge porn. Automated moderation systems, including algorithms for identifying improper content, include shortcomings that often lead to delayed removal of sensitive items. Moreover, there often exists an absence of explicit norms or the enforcement

of current regulations regarding the dissemination of revenge porn, facilitating its continuation and proliferation.

- Cultural factors contribute to the proliferation of revenge porn. In some countries characterized by gender inequity and patriarchal ideals, women often exhibit heightened vulnerability to such assaults. Social media serves as a conduit for cyber exploitation, whereby revenge porn is used as a tool to degrade or dominate people, particularly women.
- The emergence of advanced technology, including deepfake software, has introduced a new facet to the spread of revenge porn. Deepfakes enable the creation of counterfeit sexual material with authentic faces, which are then disseminated over social media platforms. This technology significantly amplifies the prevalence of detrimental information and complicates victims' ability to protect themselves.

The **consequences** of the Proliferation of Revenge Porn via Social Media are as follows-

- Individuals subjected to revenge porn endure significant psychological repercussions, including anxiety, despair, and post-traumatic stress disorder (PTSD). The public aspect of social media sometimes exacerbates these mental health difficulties, since photographs or videos may be extensively shared and subjected to commentary by unfamiliar individuals.
- Victims of revenge porn may encounter considerable social shame, especially in areas where conventional gender roles and norms dominate. Instead of making offenders responsible, victims may be reproached for producing or disseminating intimate information first.
- Revenge porn incurs significant economic repercussions for victims. Sharing intimate stuff on social media may result in job loss, harm to professional reputation, and difficulties in future career opportunities. Numerous businesses exhibit reluctance to hire people whose private photographs have been disseminated online, seeing them as potential liabilities or catalysts for public controversy.
- Despite the proliferation of regulatory frameworks aimed at combating revenge porn, implementation remains uneven across various countries. In several nations, there are no explicit laws governing non-consensual pornography, resulting in victims lacking legal remedies. Where legal safeguards are available, victims may confront the supplementary obstacle of manoeuvring through intricate, protracted legal procedures while persistently experiencing public humiliation.

ASSESSING INDIA'S LEGISLATIVE FRAMEWORK: A QUESTION OF ADEQUACY

BHARATIYA NYAYA SANHITA

There are some sections of the Bharatiya Nyaya Sanhita that are used in instances of revenge porn, despite the legislation not directly mentioning it. The following parts are of utmost relevance: ***Section 77 (Voyeurism):*** This provision criminalizes voyeurism, defined as the act of seeing or recording a woman engaged in an intimate act without her agreement. This section mostly addresses the act of recording but may also include some elements of revenge porn.

Section 356 (Defamation): Revenge porn often inflicts damage on the victim's reputation, and defamation may be used to punish the offender. Nonetheless, defamation is often treated as a civil issue and fails to adequately confront the criminal aspects of revenge porn.

Section 79 (Insulting the Modesty of a Woman): This provision criminalizes the act of insulting a woman's modesty by verbal, gestural, or physical means. Although applicable to instances involving the sharing of explicit photographs or films, its relevance in the digital world is limited.

Section 78 (Stalking): This provision may be applied if revenge porn is used to harass or stalk a victim online. It criminalizes both physical and cyberstalking, recognizing the rising problem of online harassment, which frequently accompanies revenge porn cases.

INFORMATION TECHNOLOGY ACT, 2000 (AMENDED 2008)

The Information Technology Act, 2000 is crucial in combating cybercrimes, such as revenge porn, due to the increase in digital offenses.

Section 66E (Violation of Privacy): This provision imposes penalties for the unauthorized capture, publishing, or transfer of a picture depicting a private region of an individual, under conditions that infringe upon privacy rights. It primarily pertains to the unauthorized dissemination of private material, making it a crucial clause against revenge porn.

Section 67 (Punishment for publishing or transmitting obscene material in electronic form): This provision forbids the dissemination or transmission of obscene content in electronic format. Section 67 was often used in revenge porn instances before to the introduction of Section 67A and Section 67B, which targeted particular issues.

Section 67A (Punishment for publishing or transmitting of material containing sexually explicit act etc. in electronic form): This provision addresses the dissemination of sexually explicit material, making it particularly pertinent to revenge porn incidents involving the unauthorized sharing of graphic recordings or photos.

The sanctions under the IT Act are stringent, with Sections 66E and 67A imposing imprisonment and monetary penalties. The difficulty is in the implementation of these regulations and the procedural lags in prosecuting cybercrimes.

PROTECTION OF WOMEN FROM DOMESTIC VIOLENCE ACT, 2005 (PWDVA)

The PWDVA mainly addresses domestic abuse but has rules applicable to revenge porn cases involving a partner or spouse. The law acknowledges several types of abuse, include emotional and mental abuse, which may arise from the non-consensual distribution of personal material.

THE CONSTITUTION OF INDIA

The Constitution of India offers extensive safeguards, including the Right to Privacy under Article 21, which was upheld in the pivotal Supreme Court ruling in ***K.S. Puttaswamy*** v. ***Union of India***. The right to privacy, especially in the digital era, encompasses the protection of persons from the unauthorized disclosure of personal information, including intimate photos or videos. The Right to Dignity, implicitly

included by Article 21, serves as a vital constitutional safeguard in revenge porn cases, enabling courts to address the significant violation of the victim's dignity in such instances.

The Indian courts have adjudicated revenge porn cases by using a blend of Penal Laws and provisions from the IT Act, drawing upon privacy and defamation statutes. Courts have often adopted a proactive approach, issuing injunctions to halt the continued distribution of obscene content and mandating platforms to remove infringing material. Significant rulings have acknowledged the profound emotional and reputational damage inflicted upon victims. In several instances, courts have contemplated recompense for the psychological distress endured by victims, establishing precedents for civil remedies in conjunction with criminal punishment. Although India's existing legal structure offers little protection against revenge porn, the lack of a separate legislation addressing this offense complicates prosecution efforts. Though India has made significant progress in combating revenge porn; but, with the advancement of technology and digital platforms, a more comprehensive and sophisticated legal framework is essential to safeguard victims and ensure accountability for offenders.

JUDICIAL RESPONSE

Some noted judgments in the area of Revenge Porn are as follows-

State of West Bengal Vs. Animesh Boxi

The defendant was found guilty of disseminating personal recordings of his girlfriend without her permission. He used the videos to extort her. The court adjudicated the accused guilty under several provisions of the Indian Penal Code (IPC) and the Information Technology (IT) Act, 2000. He was found guilty under IPC Sections 354C (voyeurism), 509 (acts designed to offend a woman's modesty), and IT Act Sections 66E (invasion of privacy) and 67A (distribution of sexually explicit information). This case represents a pivotal moment in addressing revenge porn in India, establishing a precedent for such offenses under the IPC and IT Act.

Sanjana Singh Vs. State of Maharashtra

The victim's graphic photographs were disseminated online by an acquaintance without her authorization. The defendant used these photographs to coerce financial gain from the victim. The Bombay High Court affirmed the conviction of the defendant for violations of Sections 354C (voyeurism), 500 (defamation), and 509 (insulting the modesty of a lady) of the Indian Penal Code, as well as Sections 66E and 67A of the Information Technology Act. The case illustrated the use of several legal measures to punish offenders of revenge porn, integrating portions from both the Indian Penal Code and the Information Technology Act for a more thorough legal approach.

Sunil Tiwari Vs. State of U.P

The defendant disseminated private images of his former partner post-relationship termination, without her authorization. The victim reported to the police, and the perpetrator was charged under many provisions of the IPC and IT Act. The Allahabad High Court underscored the need of protecting human dignity and privacy in digital environments and hence refused bail to the defendants. This case is crucial

in establishing that the non-consensual dissemination of personal material may incur substantial legal repercussions under Indian law.

Swati Vs. State of Rajasthan

The defendant disseminated private, personal photographs of his ex-girlfriend online, resulting in significant psychological distress for the victim. The Rajasthan High Court mandated prompt action against the offenders and ordered the eradication of any explicit information from the internet. This case underscores the need of prompt court action to remove revenge porn material from web sites.

XYZ Vs. State of Maharashtra

A lady filed a complaint against her former partner for disseminating her private images and videos on a social networking site. The data was disseminated post-relationship termination and used to malign her character. The court deemed the accused culpable under IPC Sections 354A (sexual harassment), 354D (stalking), and other sections of the IT Act, mandating the prompt removal of the objectionable content. This case demonstrates the judiciary's promptness in addressing cybercrimes against women, namely the expedited removal of detrimental information.

ROLE OF SOCIAL MEDIA IN PREVENTING REVENGE PORN AND CHALLENGES FACED IN DEALING WITH REVENGE PORN

The Role of Social Media in Mitigating Revenge Porn –

- In reaction to increasing public awareness and legal pressure, several social media sites have established regulations to restrict the dissemination of revenge porn. Facebook, for instance, used "PhotoDNA" technology to identify and obstruct the uploading of personal photographs without authorization. Platforms have established reporting systems enabling users to identify and request the removal of non-consensual material.
- Social media platforms may function as an effective instrument for increasing knowledge about the detrimental effects of revenge porn and instructing users on self-protection measures. Initiatives like "#EndRevengePorn" and "Stop the Steal" have used social media to promote discussions on consent, digital privacy, and online abuse.
- Social media sites have started to integrate artificial intelligence (AI) and machine learning technology to detect and eliminate non-consensual pornographic material. However, artificial intelligence has not yet achieved the ability to completely comprehend the context in which personal information is disseminated, and it often has difficulties in distinguishing between consenting and non-consensual material.
- Numerous sites have included mechanisms enabling users to report revenge porn and other detrimental material. Furthermore, several platforms now enable users to pre-emptively inhibit the distribution of personal photographs by submitting them to a secure database, therefore preventing others from posting the same images. Nonetheless, these methods often depend on the victim's proactive actions.

- Social media may positively contribute to increasing awareness of revenge porn and promoting enhanced safeguards for victims. Activists and advocacy groups have used these forums to organize campaigns, advocate for legislative reforms, and provide services for persons impacted by revenge porn.

The **challenges** faced by the Social Media in preventing Revenge Porn are as follows-

- The vast amount of material shared on social media platforms every second complicates the real-time monitoring and detection of revenge porn incidents. The contagious nature of social media allows detrimental information to proliferate swiftly before platforms can take action.
- Detecting revenge porn is intricate due to the fact that it often entails stuff made consensually yet disseminated non-consensually. Distinguishing between authentic adult content and fraudulently disseminated private material is challenging without infringing on privacy rights or using intrusive surveillance methods.
- End-to-end encryption on platforms like WhatsApp or Messenger hinders the capacity to monitor and trace the dissemination of revenge porn. Although encryption is crucial for user privacy, it also hinders platforms from accessing and filtering potentially dangerous information sent over private messaging.
- Offenders often use anonymous or fictitious accounts to disseminate revenge pornography, complicating the ability of platforms to identify and address the culprits. Despite account deletions, individuals may effortlessly establish new profiles to continue in their activities.
- Numerous victims of revenge porn refrain from reporting the material due to stigma, humiliation, or fear of more harassment, hence hindering or obstructing platforms from taking action. This creates an obstacle for social media corporations to act effectively.
- Although platforms use both human and machine moderators to identify and eliminate hazardous material, the moderation process may be sluggish and erratic. Automated technologies may inadequately identify revenge porn, whilst human moderators often experience an overload of complaints.
- Despite sites removing revenge porn, offenders may swiftly re-upload the material or disseminate it across other channels. The "whack-a-mole" issue complicates platforms' ability to comprehensively regulate the dissemination of hazardous information.
- The emergence of deepfake technology introduces a novel aspect to revenge porn, whereby fabricated intimate photographs are produced via artificial intelligence. Social media networks have difficulties in identifying and eliminating these advanced types of material, since they may be very challenging to differentiate from authentic photographs.
- Platforms must reconcile the need of damage prevention with the safeguarding of free expression. Excessive content removal procedures may result in allegations of censorship, whilst insufficient enforcement might permit the spread of dangerous material such as revenge porn.

CONCLUSION AND RECOMMENDATIONS

Social media, due to its extensive reach and ease of content distribution, paradoxically contributes to both the proliferation and the mitigation of revenge porn. Platforms like as Facebook, Instagram, Twitter, and Snapchat may serve as conduits for the rapid dissemination of explicit non-consensual photographs and videos, exacerbating privacy violations and intensifying the suffering inflicted upon victims. Conversely, these platforms have the capacity to serve as crucial partners in the prevention, detection, and mitigation of revenge porn via enhanced rules, technology, and support systems. The dual function of social media stems from its open framework, which allows malevolent users to abuse freedoms. When properly controlled and integrated with successful collaborations with legal authorities, social media platforms may serve as a formidable bulwark against revenge porn.

RECOMMENDATIONS:

- There is an imperative need for standardized worldwide regulations across all social media platforms to combat revenge porn and other manifestations of image-based abuse. Social media businesses must assume more accountability for user-generated material and enhance their algorithms to proactively identify and report revenge porn. Legislation addressing revenge porn must be consistently revised to accommodate the changing dynamics of internet harassment.

- Platforms need to invest in advanced AI technologies capable of real-time detection of revenge porn. These systems must identify even modified or altered photographs using deep learning principles, so thwarting offenders from manipulating images to evade detection. The reporting systems on platforms must be enhanced for convenience and clarity, enabling users, especially victims of revenge porn, to flag material without facing a lengthy and complex procedure.

- Campaigns aimed at enhancing digital literacy may educate people about the risks associated with sharing intimate information and the possible exploitation of such material. These efforts may also inform users about reporting channels and legal safeguards accessible to victims of revenge porn.

- Social media platforms have to engage with NGOs and governmental entities to provide timely assistance to victims of revenge porn. This may include helplines, legal aid, and mental health services accessible immediately on the site after the reporting of an occurrence. A streamlined process for revenge porn lawsuits would provide victims with expedited resolutions.

- Social media businesses have to enhance their cooperation with law enforcement organizations to identify offenders and provide essential data for criminal investigations. Law enforcement must undergo specific training to manage revenge porn cases, including knowledge of the technology and social media platforms involved, as well as collaboration with platform operators to properly collect evidence.

*****

AI IN INDIAN HIGHER EDUCATION: TRANSFORMING LEARNING WHILE NAVIGATING ETHICAL AND LEGAL CHALLENGES

Matisa Majumder[27] and Sonali Gurung[28]

ABSTRACT

Artificial Intelligence (AI) has quickly emerged as a game-changer for worldwide education, altering learning is given and administered. In India, Ai's potential in education is especially important with adaptive learning platforms and administrative tools that can improve both teaching efficiency and student success. However, as India becomes a leader in AI adoption, it faces unique challenges including ethical concerns around data privacy and algorithm bias, intellectual property rights, and exacerbation of socio-economic disparities. This paper explores the integration of AI in higher educational institutions, focusing on tools such as personalized learning platforms, administrative management systems, and natural language processing (NLP) applications chatbots. It also discusses a few key government initiatives, such as the National Educational Policy (NEP) 2020 and National Strategy on AI by NITI Aayog, which aim to promote AI's use in education while addressing the digital divide. Furthermore, this study examines the ethical and legal implications of AI usage, particularly regarding data protection, intellectual autonomy, and the evolving landscape of intellectual property laws. With case studies from Indian institutions and recent judicial decisions, this article emphasizes the importance of balanced AI deployment that promotes fairness, openness, and inclusivity. By addressing these concerns, AI could serve as a powerful instrument for improving education access and quality while protecting the rights of educators and students in India.

Keywords: Artificial Intelligence (AI), Higher Education, Ethical Considerations, Data Privacy, Intellectual Property.

INTRODUCTION

Education has evolved in response to technological advancements, with the introduction of digital media followed by access to e-books, online publications, news, and journals. The latest digital revolution offered by Artificial Intelligence (AI) is altering numerous sectors and education is one of them. The potential for AI in education is enormous. AI-powered adaptive learning platforms can generate individualized experiences that adapt to each student's unique needs. By identifying learning experiences that meet each student's specific needs. Beyond classroom restrictions, AI can act as an important support tool in countries such as India where a high student-to-teacher ratio is a concern. Through platforms such as Byju and Vedantu, the Indian education sector is rapidly using AI to provide personalized learning experiences to millions of students, particularly in rural areas. These AI tools are helping to bridge the gap between urban and rural education by offering scalable solutions that reach underserved regions. In addition, AI-driven Enterprise Resource Planning (ERP) systems optimize administrative functions like scheduling curriculum management and student performance analytics in schools and universities. However, challenges such as socioeconomic disparities, data privacy, and

[27] Senior Legal Analyst at Contract and Compliance Management, London, United Kingdom.
[28] Ph.D Candidate, Faculty of Architecture, CEPT, Ahmedabad, India.

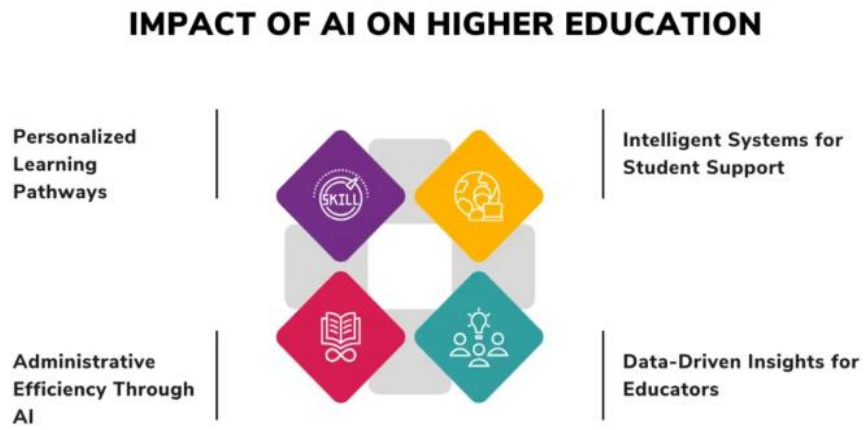
algorithm bias remain significant concerns. Therefore, to fully harness AI's potential in India, addressing these ethical and regulatory issues is essential, ensuring AI benefits are accessible to all.

AI IN EDUCATION: TRANSFORMING LEARNING IN INDIA

In education, AI is proving to be transformative, driving innovation in institutional methods, and enabling personalized learning experiences by elevating student engagement making these learning processes more efficient, adaptive, and impactful. With one of the largest networks of higher education institutions worldwide, India plays a significant role in the global education sector. India had 41.38 million students enrolled in higher education in 2020–21, according to the IBEF report. Furthermore, between 2021 and 2022, the nation's online education market is expected to grow by US$2.28 billion.

Figure 1 Impact of AI on Higher Education

Source: Eklavya- NGO that develops and field tests innovative educational programmes



A few roles being catered by AI within the landscape of education are:

1. ***Automation of Administrative Task:*** A Deloitte survey revealed that 67% of education leaders believe AI will assist with tasks such as admission, grading, and managing student records by reducing educators' administrative load and improving accuracy and efficiency. According to the World Economic Forum, integrating AI into administrative work could cut the time spent on routine tasks by 20%, enabling teachers to devote more attention to teaching and mentoring students.
2. ***Enhancing engagement and empowering learners:*** Immersion-based learning is facilitated by technologies such as AR and VR, and instant academic support is provided by AI-powered chatbots and visual assistants that respond to queries and offer advice. This facilitates students' active engagement, leading to increased involvement and a more profound understanding of intricate ideas..
3. ***Gratification and Interactive Learning:*** According to a Markets and Markets report, the global market for satisfaction in education is expected to grow at a compound annual growth rate (CAGR) of 32.0% to reach USD 3.5 billion by 2025. Artificial Intelligence (AI) facilitates the

development of intelligent educational games that adjust to the proficiency and development of individual students by improving comprehension and retention.

4. ***Data-driven insights:*** AI analytics provides critical insights into student performance and learning behaviour. Teachers can leverage this data to pinpoint areas for improvement, adjust their teaching methods, and deliver more personalized support. However, educational institutions must also be mindful of the potential downsides of AI in learning environments.

AI tools and technologies used for Education in India

A few AI tools for students and teachers include Grammarly, which enhances writing clarity and correctness, and QuillBot, a paraphrasing tool that helps avoid plagiarism. Canva aids in creating visually appealing presentations with an intuitive UI/UX design, and Wolfram Alpha provides AI-powered answers across various subjects. Gradescope assists teachers with efficient grading feedback, leveraging AI to streamline the process, while Tutor.ai provides personalized tutoring. Other useful tools are Research Rabbit for discovering scholarly publications and Google Lens, which identifies photos and text for study purposes. These AI-powered solutions, combined with user-friendly UI/UX design, significantly enhance learning and simplify both academic and administrative tasks. Key tools such as Adobe and Figma now incorporate AI plug-ins which automates tasks and suggestions enhancing the creative landscape and building a new generation of designers. These AI tools incorporated in Indian educational platforms assists the students and the educators that intends to ease out the educational learnings.

Legislative Policies Impacting AI in Higher Education

Indian legislation is evolving to keep pace with technological advancement. The government of India has enacted various policies to foster technology-based innovation, particularly in the context of AI.

(A) National Educational Policy 2020 (NEP 2020) and AI's Impact

The National Education Policy 2020, aims to integrate technology, including AI, to transform the educational landscape in India. Key initiatives under NEP 2020 that utilize AI include:

- National Educational Technology Forum (NETF) that facilitates discussions on technology usage in education.
- E-Learning Platforms such as SWAYAM, NPTEL, and DIKSHA leverage AI-driven research and development to provide quality educational resources to a diverse student body.
- Academic Bank of Credit (ABC), employs AI to track student progress and enable credit transfers among institutions.

Therefore, NEP2020 aligns with the digital India initiative by promoting AI research in education, training educators in AI tools, and incorporating AI literacy into the curriculum to prepare students for an AI-driven future.

(B). AI Adoption in NITI Aayog

NITI Aayog is India's primary policy think tank, and plays an important role in promoting AI adoption. In 2018, it launched the National AI Strategy, which focuses on using AI to address socioeconomic challenges.The initiatives aim to improve AI literacy and facilitate educators' continuous professional development, allowing for effective technology integration in the classroom.

Key initiatives are:

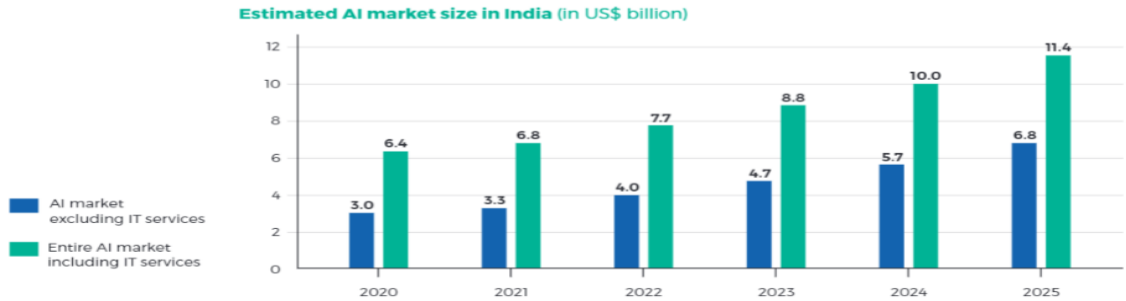
- National Strategy for Artificial Intelligence (NSAI), emphasizes using AI for personalized learning and enhancing student engagement.
- Atal Innovation Mission (AIM) through Atal Tinkering Labs (ATL) in over 5000 schools, encourages exploration in AI and technology-based innovations to promote Science, Technology, Engineering, and Mathematics (STEM) education and hands-on learning.
- AI for All in collaboration with Intel and other partners, boosts AI literacy among students and educators by enhancing the understanding of AI fundamentals and applications.

As a result, NITI Aayog encourages the development of AI-powered platforms for personalized learning, which will help to fill educational gaps and improve learning outcomes.

(C). Relevance of AI literacy in Indian Education

Both the NEP 2020 and NITI Aayog's strategies highlight the significance of AI literacy in shaping India's future, particularly given that over half the population is under 25. While elementary enrollment is high at 97%, retention rates are concerning with only 70.7% at the elementary level and 57.4 % at secondary schools. Factors contributing to these issues include multi-grade classrooms, rote learning, inadequate support for dropouts, and ineffective teacher training. Despite global EdTech spending reaching USD 160 billion in 2016, India's adoption is slow due to limited teacher training and student and educator resistance. AI offers solutions through adaptive learning tools, intelligent tutoring systems, and predictive models to identify at-risk students. Initiatives like Microsoft's collaboration with the Andra Pradesh government exemplify AI's potential to enhance educational outcomes. NITI Aayog recognizes the urgent need for AI literacy, suggesting reskilling the workforce and prioritizing AI-related subjects in education from primary to secondary levels. As of August 2020, the value of India's AI reached US $6.4 billion, with expectations for steady growth, highlighting the need for a workforce equipped with AI skills. Fig 2, illustrates how a steady growth of this market is expected in the following years.

Fig-2 NITI Aayog forecast on growth of AI in market in India



Source: Analytics India Magazine and Jigsaw Academy, 2020

(D) Government initiative for AI learnings in Indian Education

The government of India is reshaping E-learning through digital learning as a long-term strategy in the education sector, expanding learning beyond schools. The Ministry of Education focuses on inclusive learning by adapting enhanced digital experiences for all students. Key initiatives are:

- ***The first AI-powered Educational Tablet:*** India's first AI-enabled educational tablet featuring BharatGPT, an AI virtual assistant that provides inter-lingual translation promoting inclusivity.
- ***Atal Innovation Mission 2016***, focuses on fostering innovation and entrepreneurship among youth with AI literacy, with 10,000 Atal Tinkering Labs (ATLs) across the nation providing training on new technologies and research.

These initiatives promote equitable learning and improve access to quality education through technology across the country. Collaborations with tech companies such as Intel and Meta. This government initiative provides valuable resources for young motivators.

ETHICAL CONSIDERATIONS REVOLVING AI IN HIGHER EDUCATION

The rapid incorporation of AI into academic institutions generates certain ethical concerns, essentially relating to data privacy, algorithm bias, and its impact on the student-teacher relationship. Additionally, the increasing reliance on AI in education risks altering traditional students' teacher dynamics, potentially weakening the personal connection and mentorship that are critical to student's development.

Ethical Challenges in India's Higher Education-

India's AI implementation in education faces unique ethical challenges due to societal disparities and cultural differences in ethical practices. AI tools are considered to have the potential to widen the gap between privileged students in urban areas and those in rural economically disadvantaged regions. We have learning platforms like Byju's which offer personalised learning experiences tailored to individual students' needs, their reach is often limited by digital literacy and access to technology in underserved areas. The Byju's model leverages advanced algorithms to create customised educational content, yet it can inadvertently exacerbate educational inequalities by favoring students who already have the resources to benefit from such technology.

Moreover , government initiatives like SWAYAM and NPTEL, have emerged to democratise education by offering free online courses to students across India. While these platforms aim to bridge the gap in the access to quality of education they also highlight ethical concerns regarding the educators-students relationship. The transition to online learning raises questions about the role of instructors, as the personalisation of education through AI tools can lead to diminished roles for teachers, transforming them to facilitators rather than active participants in the learning process.

Studies revolving ethical concerns on leveraging AI in Higher Education-

In India, certain studies show that while AI-driven platforms can augment learning engagement, they often come with dilemmas. A report by the TOI dated October 5, 2024, highlighted the data privacy concerns related to educational apps, indicating that many platforms collect sensitive student

information without adequate safeguards. This raises questions about how this data and who has access to it, necessitating strict regulatory frameworks to protect student privacy.

Algorithm bias in AI systems used in education is another pressing concern. A research report by the University Business School, Punjab University, Chandigarh, published in January 2020, found that biassed algorithms could disproportionately disadvantage marginalised communities, affecting their admission prospectus and academic success. This bias is often rooted in the data used to train these algorithms, which may not adequately represent the diversity of India's student population. Furthermore, the ethical considerations in education extend beyond data privacy and algorithm bias. Another study by Indian scholars examined the changing dynamics of the educator-students relationship in the age of AI, suggesting that the reliance of AI tools may lead to diminished sense of agency among students. This shift in educational philosophy poses significant ethical challenges, as it may undermine the critical thinking and problem solving skills vital for succeeding in the current world.

LEGAL IMPLICATIONS OF AI USAGE IN HIGHER EDUCATION

The surging integration of AI in academic education presents a range of legal implications, mainly concerning data privacy, intellectual property (IP), and academic integrity in India.

India's Personal Data Protection Bills (PDPB), 2019-

Currently under the review, India's Personal Data Protection Bill seeks to regulate the collection, storage and processing of personal data. Drawing inspiration from GDPR, the Bill introduced India-specific provisions, categorising data into personal, sensitive and critical types. The Bill categorised data into personal, sensitive and critical personal data, placing obligation on the data fiduciaries to ensure transparency, accountability and security in data processing.

AI technologies often rely on vast datasets, which raises concerns about privacy and the potential misuse of personal data. The PDPB's focus on purpose limitation and data minimization directly affect AI's development, as AI systems must balance their need for data and strictly regulatory requirements. AI algorithms may process sensitive personal data (such as biometric and health data), making **Section 15** and **16** of the Bill, which deal with sensitive data handling, particularly relevant data. AI-driven businesses must ensure compliance with these provisions when such data is being used. Although this Bill is not yet enabled, the government is prioritising its passage due to the increasing significance of data-driven businesses and AI applications in India.

Intellectual Property Laws and AI in India-

With AI driving innovation in education, the Indian nation is also changing with time and reviewing its existing IP legislations to accommodate these AI generated works and inventions. IP laws such as the Patent Act, 1970 and Copyright Act, 1957, are being analysed to address new challenges posed by AI tools. Particularly linked to ownership of AI-generated content and inventions pose critical legal concerns, specifically regarding authorship and inventorship when AI plays a major role in creation. The important provisions impacted by AI are-

- **Section 6** of the **Patent Act, 1970**, specifies that a patent can only be granted to a natural person or legal entity, raising questions about whether AI systems can be considered as an "inventor" for such research being done by students or educators using AI tools.
- **Section 3(d)** of **Patent Act, 1970**, prohibits patents for algorithms per say yet AI-driven inventions that incorporate algorithms could qualify if tied to a specific industrial application. This is still an ongoing discussion on AI and patents and its real impact on the provision is yet to be ascertained.
- **Section 13** of the **Copyright Act, 1957**, gives protection to original work of authorship, however the questions remain whether AI-generated content qualifies for the protections and if so who would be credited as the "author". With more educators as well as students using AI tools for research works, the aspect of AI and copyright authorship poses serious concerns on the ownership.
- The **Doctrine of Sweat and Brow** states that copyright protection can be granted to works that require significant effort; however, the doctrine becomes complex when applied to works generated autonomously by AI, where human efforts are minimal or non-existent.

As the current existing legal frameworks pose certain concerns with the changing times, the Ministry of Corporate Affairs and the Department of Industrial Policy and Promotion is in consultation on developing new frameworks to ensure adequate protection of AI related intellectual property. This includes complex issues surrounding ownership when AI creates products and handling of patents of AI-driven inventions.

JUDICIAL PERSPECTIVES ON POSSIBLE AI CHALLENGES IN HIGHER EDUCATION

A few landmark judgements by India courts, which seems to be farsighted and help us understand the possible challenges arising out of AI usage in higher education.

Copyright Ownership highlighted in *Vivek Kumar v. U.P. Power Corporation Lid. (2021)*-

In this case, the Allahabad High Court dealt with copyright issues surrounding educational materials. Vivek Kuamr, an educator, claimed that his original teaching material including lecture notes and presentations had been copied without permission by the U.P. Power Corporation for use in their training programs.The Court ruled in favour of Kumar, emphasising the importance of protecting origination education content form unauthorised use, This ruling is significant in understanding the implications of AI usage poses in higher education, particularly as institutions rely on AI tools to generate and distribute educational materials. The judgement reinforces the need for universities and educational institutions to respect copyright laws and ensure that any AI-generated content based on educators original materials is appropriately licensed and accredited.

Technology usage in Education Emphasised in *The State of Maharashtra v. The State of Gujarat (2020)*- This case addressed the legality of e-learning during the coronavirus pandemic. The Maharashtra government issued guidelines for online classes, including safety mandates, privacy measures and equitable access of technology to students. These guidelines were challenged by the

Gujarat government, but the supreme Court upheld the Maharashtra regulations, emphasising the importance of lawful practices in implementing technology in education. The importance of this ruling in the AI context is for highlighting the relevance of standards in use of technology in educational settings. With AI technologies being integrated into digital learning platforms , educational institutes need to ensure compliance with legal frameworks which protect students rights and privacy. This ruling encourages the development of AI usage along with prioritising ethical considerations , promoting equitable access to education.

Rights of Educators in Virtual Education Platforms accentuated in *Isha Karan v. AAI (2021)*- In this case, educators challenged a virtual education platform policy that restricted the sharing of course material outside the platform. The Delhi High Court ruled in favour if the educator affirming the rights of educators to disseminate their academic materials while noting the need to respect copyright laws and proprietary agreements, This case is critical to comprehend the evolving landscape of Ai, as it allows educators to share AI-generated or enhanced teaching materials beyond the confine of specific platforms. However the ruling also emphasised the need for clear agreements regarding ownership and rights related to AI-generated materials, using the educators to retain control over their intellectual contributions.

CONCLUSION

The journey towards an AI-driven education system is not only about the technology, but also about reimagining how knowledge is transmitted and received, and how we educate future generations for the completion of a more digital world. In India, the integration of AI into education sectors has marked a transformative era, offering unprecedented opportunities for personalized learning that have helped enhance education outcomes. Initiatives such as PM E-Vidya, DIKSHA, and the NEP 2020 show a commitment to using technology for inclusive education. But, as AI technologies and platforms emerge they have potential to address significant challenges, such as high student-to-teacher ratio and disparities in education access, particularly between the rural and urban areas. As we embrace these advancements, it is critical to remain vigilant about the ethical and legal implications. Existing legislative frameworks and ongoing discussions about intellectual property rights must adapt to protect students and educators equally. The success of AI in education is dependent on establishing a balance between innovation and ethical responsibilities. Therefore, the concerns regarding data privacy, algorithm bias, and the shifting dynamics of the educator-student relationship demand regulatory reform. Therefore, by addressing these challenges, it is believed that India can anchor the full potential of AI, ensuring that the benefits of technology are accessible to all, and fostering a more equitable and effective educational landscape.

*****

REFERENCES

- Krishna Kanta Roy, *Digitalisation in Education: Can AI Bridge India's Digital Divide?*, NORRAG Global Education Center, Geneva Graduate Institute" (Aug. 24, 2024), available at: https://www.norrag.org/digitalisation-in-education-can-ai-bridge-indias-digital-divide/
- Gurumurthy Kasinathan & Yogesh K S, *Exploring AI in Indian School Education*, IT for Change (Mar. 20 2019), available at: https://itforchange.net/sites/default/files/2019-08/Paper-AI-and-education-Seminar-by-UOH-March-20-2019-with-abstract.pdf.
- Divya Chopra, *How AI is a game changer in the education sector*, India Today (Dec. 18, 2023),available at: https://www.indiatoday.in/education-today/featurephilia/story/ai-game-changer-education-sector-2477394-2023-12-18.
- Editorial, *Government initiatives for Digital Education in India*, The Times of India (Oct. 1, 2022). available at:https://timesofindia.indiatimes.com/education/online-schooling/government-initiatives-for-digital-education-in-india/articleshowprint/94532897.cms.
- Saurav Pandey, *Top 10 AI Tools for Students & Teachers*, The Times of India (Oct. 15, 2023) available at: .https://timesofindia.indiatimes.com/education/web-stories/top-10-ai-tools-for-students-amp-teachers/photostory/104441238.cms
- Atal Innovation Mission, *NITI Aayog and Meta join hands to establish Frontier Technology Labs in schools to democratize access to future technologies and innovation*, Press Information Bureau (2024), available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2 011896
- *National Strategy for Artificial Intelligence*, NITI Aayog (2018), avialable at: https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.
- Soenke Ziesche & Kushal Kumar Bhagat, *State of the Education Report for India 2022 Artificial Intelligence in Education,* UNESCO, New Delhi (2022), available at: https://digitallibrary.in.one.un.org/.
- Sumit Tripathi & Joanna Rosak-Szyrocka, Impact of Artificial Intelligence on Society, CRC Press (2024).
- Jyoti Verma, *Digitalisation of Education: Growth Signs for EdTech Ecosystem,* Digital Analytics Applications for Sustainable Summit Training and Education, Apple Academic Press, pp. 29-42 (2025).
- Harihara Bhesera & Shankar Lal Bika, *Access, Equity and Quality in Higher Education: Envisioning India Through Swayam*, A US-China Education Review, Vol 14, No.1, pp. 11-17 (Jan. 2024), available at: https://doi.org/10.17265/2161-623X/2024.01.002.
- Mr. Balbir Singh & Dr. Meenakshi Malhotra, *The Role of Artificial Intelligence in the Indian Education Sector*, OORJA , Vol. 18, pp-21-23 (Jan.-Jun. 2020).
- Editorial, *For minorities, biased AI algorithms can damage almost every part of life*, The Economic Times (Aug. 29, 2023).

- Afiya Jamal,Anmol Pattanaik, Ravi Gorli, Ayes Chinmay & Jaisai Tenepalli, *The Impact of AI Chatbots on Teacher-Student Relationships in Higher Education*, European Chemical Bulletin, Vol.12, pp.-2651-2655 (2023), available at: https://doi.org/10.48047/ecb/2023.12.10.1822023.01/08/2023.
- Mrinal Dutta,*The Ethical Complications: AI and Autonomous Systems in a Globalized World with a Focus on India*, The Academic- International Journal for Multidisciplinary Research, Vol. 2, Issue 8 (Aug. 2024), available at: https://theacademic.in/wp-content/uploads/2024/09/50.pdf.
- G R Raghavender & Gurujit Singh, *Can Artificial Intelligence (AI) Machine be Granted Inventorship in India?*, Journal of Intellectual Property Rights, Vol. 28, pp. 123-131 (Mar. 2023), available at: https://doi.org/10.56042/jipr.v28i2.1268.
- Kumar Shahi Sarvesh, Divya Singh Rathor & Athreya H. Sundar,*A study on the protection of copyright in an AI-driven world, In AIP Conference Proceedings,* Vol. 3000, No. 1, AIP Publishing (2024).
- C.Hemavathy, *Intellectual Property Rights and Copyright Laws in the regime of Artificial Intelligence (AI) in India*, Library of Philosophy and Practice, pp 1-11 (2024).

*****

AI-DRIVEN ROBOTICS: NAVIGATING CYBER SECURITY CONCERNS AND THE RISE OF CYBERCRIMES

Shubha M.[29]

ABSTRACT

Robotics' use of artificial intelligence (AI) has transformed several sectors by increasing productivity and creativity. But this has brought up serious cybersecurity issues. As AI becomes more and more used, vulnerabilities are revealed that can be used by bad actors to commit cybercrimes. This study examines the relationship between cyber security and robots driven by AI, revealing both new risks and possible advantages. Healthcare, manufacturing, autonomous cars, and military are just a few of the areas that are using AI-driven robots more and more. However, these machines also come with security dangers, such as ransomware attacks, data breaches, and remote manipulation. The difficulty of guaranteeing system security and integrity is made worse by the absence of legal frameworks and the quick development of technology. This study investigates the cyber security of AI-driven robots, emphasizing the ways in which risks are changing, cybercriminal techniques, and the consequences for both persons and companies. The main issues that need to be addressed are data manipulation, control over robotic systems, and illegal access, all of which present threats to personal safety, security, and privacy. In order to defend AI-powered robotic systems from cyberattacks, the report highlights the necessity of proactive cyber security measures, such as strong encryption, frequent software upgrades, safe network setups, and AI-driven threat detection techniques. It also emphasizes how important it is for researchers, industry executives, and legislators to work together to create moral guidelines and laws governing the use of AI in robots. AI-driven robots have a lot of promise, but realizing that potential will require resolving cyber security issues. Society can take use of the advantages of robots driven by AI while preventing cybercrimes by recognizing and reducing risks.

Keywords: robotics, cybersecurity, cybercrimes, legal frameworks, privacy, measures

INTRODUCTION

Artificial Intelligence and robotics are changing our daily lives and various sectors such as healthcare, defence, manufacturing, logistics and transportation. The AI-driven robots can perform complex tasks and it does not require any human intervention as a result of which it is capable of making its own decisions. But one does not know how a man-made machine is able to function on its own. While this is termed as ‘black box’ being present in the AI system, it is unclear about the inside mechanism. From courtroom robots to autonomous vehicles, the growth of artificial intelligence has shaped the human lives by impacting the way we live, work and interact. This rapid advancement poses threats especially in the area of cybersecurity.

As robots are interconnected to networks and rely on large data, it makes them highly vulnerable to cyber threats. This means that the security risks are changing beyond hacking. Various cybercrimes are being committed by these AI-driven systems by exploiting people around the world. The AI systems in robots can be influenced to perform dangerous acts. While AI is being incorporated within cybersecurity to combat cyber threats, today it stands as a dangerous concern in the realm of digital world. This issue

[29] Student at Christ Academy Institute of Law, Bengaluru, India.

demands urgent attention to ensure public safety. The major difficulty lies in the formulation of a legal framework to govern the AI-driven cybercrimes or threats. While it is problematic and involves various hurdles in doing so, but it is possible to hold the person accountable if an effective legislation is passed. AI driven methodologies are recently becomes highly upgrading the industrial robotic system and its easier for factories and industries to implement the robotic system easily and inexpensive.

METHODOLOGY

This paper uses a comprehensive methodology the analyse the role of AI-driven robotics in cybersecurity which comprises of relevant literature, case studies and reports. This methodology focuses to examine the growing cyberthreats and incident response as well. The below mentioned steps are included in the methodology of this paper.

1. **Case Studies:**

This study examines real-world case studies and use cases showcasing AI deployment in cybersecurity, analysing successful implementations, challenges, and lessons learned from AI-driven solutions.

2. **Data Collection and Analysis:**

The study compiles data sources related to AI-driven cybersecurity research and applications, using statistical analysis and data visualization techniques to gain insights and trends on the effectiveness and impact of AI in cybersecurity.

3. **Framework Evaluation:**

The study evaluates existing frameworks and methodologies for integrating AI into cybersecurity practices, conducting a SWOT analysis to identify best practices and areas for improvement in AI-driven cybersecurity approaches.

THE ROLE OF AI-DRIVEN ROBOTICS IN MODERN CYBER SYSTEM

Robotics powered by AI is transforming technology and improving the capabilities of contemporary cyber systems in a variety of sectors. These days, these robots are essential to digital ecosystems that depend on autonomous behaviour, data processing, and decision-making. But there are additional difficulties brought forth by this merging, especially in cybersecurity. Managing risks and benefits in contemporary cyber systems requires an understanding of the role played by AI-driven robots. As AI advances to a higher intelligence level, more human service employees and human intelligence (HI) at the intelligence levels lower than that level should be used less.

Definition

AI-driven robots carry out tasks either fully or partially on its own by utilizing AI methods such as computer vision, deep learning, and machine learning. These robots are able to sense their surroundings, make judgments in real time, and adjust to changes by using data. To carry out intricate operations in the cyber environment, they communicate with digital systems such as sensors and cloud platforms. Self-driving automobiles, robotic industrial arms, and autonomous drones are a few examples. These

systems are essential parts of contemporary cyber ecosystems since they depend on safe cyber infrastructures for data processing, communication, and job execution.

The Role of AI in strengthening Cybersecurity

By creating sophisticated Intrusion Detection Systems (IDS) that continuously scan networks for anomalous activity or threats, artificial intelligence (AI) can improve cybersecurity. Without human assistance, AI-driven systems are capable of automatic patching, which finds and fixes flaws in robotic software. By examining historical attack trends, AI can also forecast future cyberthreats, allowing for proactive protection measures.

Major Applications and their Role in Cyber Systems

Patient care is being revolutionized by AI-powered surgical robots, robotic nurses, and diagnostic gadgets that rely on real-time data sharing between sensors, AI algorithms, and medical records. Examples of AI-driven robotics in cyber systems include self-driving automobiles, autonomous vehicles, and autonomous drones and ground vehicles. To traverse roadways, communicate with other cars, and avoid obstacles, these systems make use of sensors, cameras, and artificial intelligence algorithms. Because defence robots depend on secure communication links and real-time AI decision-making, they are both strong and susceptible. Robots that can learn and adjust to changing settings are expanding automation in factories and supply chains, increasing productivity and decreasing human error.

CYBERSECURITY THREATS IN AI-DRIVEN ROBOTICS

Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace. AI-driven robots are rapidly being incorporated into a variety of industries, including manufacturing, healthcare, transportation, and defence. This brings with it both potential and hazards. These robots are appealing targets for hackers because of their reliance on AI algorithms, networked systems, and large volumes of data, which makes them susceptible to cybersecurity attacks.

- **Malware and Ransomware Attacks**

Robotic systems are susceptible to ransomware and virus assaults, which can seriously impair their functionality. Hackers can take control of functionality, steal data, and initiate other attacks by infecting software using malware. Particularly, ransomware is becoming a more serious menace as hackers target vital systems in hopes of making big profits. For example, hackers might interrupt robotic manufacturing processes and lock down software in autonomous cars, resulting in large financial losses.

- **Supply Chain Attacks**

Supply chain assaults are a new hazard to AI-driven robotics. During production or transportation, cybercriminals may target robot hardware or software, creating backdoors that let them gain access to operations. Because these assaults are hard to identify and happen before the robot enters its operating environment, it is essential for businesses to make sure their supply chains are secure.

- **Data Breaches and Privacy Concerns**

AI-driven robots, particularly in healthcare and finance, handle sensitive data, which can be accessed, stolen, or manipulated by hackers. This data can lead to identity theft, corporate espionage, or reputational damage. The real-time data collected by these robots increases the attack surface. Inadequate encryption, insecure storage, and weak access control mechanisms can contribute to data breaches in AI-driven robotics.

- **Network and IoT Vulnerabilities**

Due to flaws in IoT devices, AI-driven robots—which are frequently incorporated into broader cyber-physical systems and IoT networks—can be subject to cyberattacks. Attackers may use these flaws, such as out-of-date software, unprotected communication protocols, or a lack of encryption, to access the robot's system. The Mirai botnet assault emphasizes how crucial it is to give network and Internet of Things security top priority in order to stop illegal access or control of AI-driven robots.

LEGAL, ETRHICAL AND REGULATORY IMPLICATIONS

Legal, ethical, and regulatory issues like as responsibility, data privacy, safety, and justice are brought about by the development of AI-driven robotics. Frameworks that safeguard users, reduce risks, and promote innovation are being developed by governments, regulatory agencies, and businesses. Ensuring data privacy, encouraging accountability, and protecting data privacy in crucial areas are important legal, ethical, and regulatory ramifications.

Legal Accountability and Liability

Determining responsibility and liability in the event of damage or failure is one of the legal difficulties in the field of AI-driven robots. The topic of who is at fault for mishaps is brought up by autonomous robots, which make choices without human input. The complicated decision-making processes of AI systems are difficult for current legal systems to manage, and the arrival of robots with different degrees of autonomy makes things even more difficult. Legal frameworks must change to clearly define accountability and responsibility in cases involving AI-driven robots. This includes constructing insurance mechanisms to cover damages brought on by robotic systems and establishing liability for particular actors involved in robot design, programming, and deployment.

Ethical Concerns in Decision Making and Bias

Due to biases in their training data, AI-driven robots that rely on machine learning algorithms may provide immoral results. This may lead to law enforcement robots unfairly targeting particular populations or healthcare robots giving some people worse than ideal treatment because of their gender or colour. Particularly in delicate fields like criminal justice, healthcare, and recruiting procedures, ethical considerations are crucial. In order to guarantee ethical AI, developers should give fairness in models top priority, check training data for bias, increase decision-making transparency, and set up explicit procedures for human supervision and decision-making process intervention.

Regulatory Frameworks for Safety and Certification

Given their growing usage in the industrial, transportation, and healthcare sectors, the safety of AI-driven robots is a critical regulatory concern. Regulatory bodies must set strict safety requirements and

certification procedures for these robots, including controlling the AI models, hardware, and software, in order to prevent injury. To avoid regulatory fragmentation and provide uniform safety and security standards, governments and international organizations must also harmonize rules across countries.

STRATEGIES AND SOLUTIONS FOR SECURING AI-DRIVEN ROBOTICS

i. Implementation of Strong Encryption and Data Protection

AI-driven robots' extensive data production, transmission, and processing capabilities make them susceptible to data theft and manipulation. Both data at rest and data in transit should use robust encryption algorithms to guard against unwanted access or manipulation with sensitive data. The robotic system operates with safe data encryption thanks to encryption techniques like AES and TLS. By limiting access to vital systems and data, access control techniques like multi-factor authentication (MFA) can lower the risk of insider threats and illegal access.

ii. Securing AI Models Against Adverse Attacks

When coming up with the long run analysis, development and application of AI ways in Cyber Security, one needs to distinguish between the immediate goals and long views. Robotic AI models are vulnerable to adversarial assaults, in which adversaries alter input data to trick the AI's judgment. By identifying and fending off hostile inputs, methods such as adversarial training can increase AI resilience. By increasing the transparency of AI decision-making, explainable AI (XAI) enables engineers to see anomalous behaviour that might indicate an attack and take preventative measures. Both techniques aid in defending AI systems from possible dangers.

iii. Regular Software Updates and Patching

Robots powered by AI depend on complex software, which may have flaws. Patching and regular updates are essential for addressing these vulnerabilities. Rapid device deployment of security updates using automated patch management systems reduces vulnerability to possible attacks, particularly in IoT networks where unpatched vulnerabilities might be widely exploited.

iv. Intrusion Detection Systems (IDS) and Real-Time Monitoring

AI-based intrusion detection systems (IDS), which continually analyse network traffic and identify questionable activities, are essential for protecting AI-driven robots. These systems can evolve over time to enhance detecting skills when paired with machine learning. Robotic systems that are monitored in real time can also identify behavioural abnormalities, enabling operators to make necessary corrections before serious harm is done. These systems can improve their detection skills by learning from previous attacks.

v. Establishing Regulatory Standards and Governance

Both technological advancements and legislative frameworks are necessary for the safe use of AI-driven robotics. In order to help businesses adopt best practices like safe coding, ethical AI use, and GDPR compliance, governments and industry associations should create cybersecurity guidelines for AI and

robots. Organizations may reduce cyber threats and ensure legal and regulatory compliance by using frameworks such as the Risk Management Frameworks (RMF), which assist in identifying, evaluating, and mitigating cybersecurity risks related to AI-driven robots.

vi. Human-Robot Collaboration in Cybersecurity

AI-driven robotics cybersecurity should be seen as a human-robot partnership, with human operators being essential in system monitoring, alarm response, and decision-making during security events. Good training initiatives may raise staff members' knowledge of cyberthreats and get them ready for security lapses. Specialists must work with AI and keep striving for its appropriate and optimal use, and not become complacent or over-reliant on third party ML-based solutions.

FUTURE TRENDS AND EMERGING RISKS

The next trend in AI-driven robotics is towards completely autonomous robots with advanced self-learning capabilities. Without human assistance, these robots are capable of making intricate judgments, learning from data in real time, and adjusting to their surroundings. But this independence makes cybersecurity more vulnerable. Cybercriminals may target robots to alter their behaviour or obtain illegal access since they interface with other networks and systems. Attackers could take advantage of flaws in AI models, which could have unexpected and harmful consequences. It is anticipated that essential infrastructure industries including energy, transportation, healthcare, and military will increasingly rely on AI-driven robots. They will carry out military operations, surgeries, and power grid management. Swarm robotics, in which several robots collaborate to accomplish complicated tasks, has promise for military operations, agriculture, and disaster relief. But there are new cybersecurity issues with this technology. Adversarial assaults are getting more complex, and machine learning algorithms for decision-making rely significantly on these techniques. Strong cybersecurity frameworks, cutting-edge AI security research, and international cooperation are required to reduce these dangers. This will assist in defending robotic systems powered by AI against changing threats.

The consequences of these emerging AI-driven cyberattacks could be life-threatening and highly destructive. By undermining data confidentiality and integrity, highly sophisticated and stealthy attacks will erode trust in organizations and perhaps result in systemic failures.

CONCLUSION

By increasing automation and efficiency, AI-driven robotics is transforming sectors including healthcare, manufacturing, transportation, and military. However, a number of cybersecurity issues are brought about by this convergence with cyber systems. Robots are particularly vulnerable to cyberattacks, such as ransomware, malware, and data breaches, since they depend on linked networks like the Internet of Things and cloud services. The research paper draws attention to certain cybersecurity issues, such as hostile assaults on AI models and flaws in data integrity and real-time communication. Case studies demonstrate how cyberattacks on industrial systems, medical robotics, and driverless cars have practical repercussions that impact both human safety and financial interests.

A comprehensive strategy is required to safeguard AI-driven robotics from cyberattacks. This covers governance strategies like modernized legislative frameworks and global cybersecurity standards in addition to technological solutions like encryption and machine learning algorithms. To create effective defences, cooperation between researchers, commercial companies, and governments is essential. To maintain the safe and efficient operation of these systems in a world that is becoming more and more digital, a proactive and cooperative approach is required. By embracing the principles of collaboration, innovation, and adaptability, organizations can stay ahead of cyber adversaries and safeguard their digital infrastructure in an increasingly interconnected and digitized world.

******

INTEGRATING ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGY IN BIOTECHNOLOGY: A COMPARATIVE ANALYSIS OF PATENT LAW AND CYBERSECURITY IMPLICATIONS IN INDIA AND USA

Avleek Dhiman[30] and Shivansh Chauhan[31]

ABSTRACT

This paper explores the integration of artificial intelligence (AI) and blockchain technology in the biotechnology sector, focusing on their implications for patent law and cybersecurity in India and the USA. As AI drives innovation in biotechnology, it poses significant challenges to existing patent frameworks, particularly concerning issues of inventorship, patentability, and intellectual property rights. Concurrently, blockchain technology offers promising solutions for enhancing transparency, security, and efficiency in patent filing and data management processes. This study conducts a comparative analysis of the legal and regulatory landscapes in India and the USA, examining how each country addresses the intersection of these emerging technologies. Additionally, it evaluates the cybersecurity risks associated with the adoption of AI and blockchain in biotechnology, highlighting vulnerabilities and potential mitigation strategies. Ultimately, this research aims to provide insights for policymakers and industry stakeholders, emphasizing the need for adaptive legal frameworks that can accommodate the rapid evolution of technology in the biotechnology field.

Keywords: Artificial Intelligence, Blockchain Technology, Biotechnology, Patent Law, Cybersecurity, Comparative Analysis, India, USA, Intellectual Property.

INTRODUCTION

Artificial intelligence (AI) and blockchain technology together are opening new boundaries in biotechnology, providing creative ideas for data administration, diagnostics, medication discovery, and more. These technologies are essential for improving the efficiency and openness of biotechnological methods, therefore supporting individualised medicine and more industry-wide cooperation. The biotechnology industry is becoming more data-driven, so artificial intelligence and blockchain clearly have great potential to improve decision-making, automate difficult operations, and secure enormous volumes of private biological data. Still, the legal systems in charge of these developments—particularly in regard to patent law and cybersecurity—cause major challenges and variances across major nations like India and the United States.

ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN IN BIOTECHNOLOGY

Artificial intelligence and blockchain are revolutionising the biotechnology industry by simplifying research and development procedures, improving data analytics, and safeguarding of private data. Accelerating drug development, genetic research, and customized care depends much on AI's capacity to examine large volumes of complicated data. Blockchain is very useful in managing intellectual property and guaranteeing data integrity in clinical trials since it provides a distributed system guaranteeing transparency, immutability, and increased security. In the context of biotechnology, blockchain guarantees the traceability of biological samples and intellectual property, while artificial

[30] Research Scholar at Gujarat National Law University, India.
[31] Assistant Professor of Law at D.P. Vipra Law College, India.

intelligence's function goes to predictive analytics, therefore enabling more accurate modeling of biological systems. Blockchain can be used, for example, to log intellectual property claims or patent filings, therefore guaranteeing that ownership and invention are exactly recorded and unchangeable. Though these technologies have great potential, their integration presents different difficulties especially in the spheres of legal protection and cybersecurity.

INDIA'S PATENT FRAMEWORK AND BIOTECHNOLOGY

The Patents Act of 1970, which has been changed multiple times to fit the expanding field of biotechnology, is the patent law controlling biotechnology developments in India. India allows the patenting of biotechnological innovations, but the legislative environment is still changing in view of fresh technical developments such artificial intelligence and blockchain. Biological inventions under Indian patent law must satisfy the general requirements of patentability—novelty, non-observance, and industrial usefulness. But Section 3(b) of the Patents Act forbids inventions that contradict public order, morality, or that entail the simple finding of a new form of a known chemical. Patenting some biotechnological innovations—especially those involving human genes or genetically modified organisms—becomes difficult this way.

In India, artificial intelligence-driven biotechnology innovations present particular challenges. Given that AI-generated ideas might lack obvious human inventiveness, issues about their patentability under the current legal system surface. Furthermore, the inclusion of blockchain technology into biotech patent applications brings complexity regarding the ownership and transfer of digital assets, which Indian law is still not completely able to handle. For entrepreneurs in this field, the lack of clear legal clauses for artificial intelligence and blockchain inside the biotechnology patent territory generates ambiguity.

THE USA'S PATENT FRAMEWORK AND BIOTECHNOLOGY

On the other hand, guided mostly by the Patent Act of 1952 and its revisions, the United States has a more developed legal environment when it comes to patenting biotechnological advances. With defined policies on the patentability of biotechnological inventions—including those produced or supported by artificial intelligence—the U.S. Patent and Trademark Office (USPTO) is more flexible in technological changes. Furthermore regarded as patentable are blockchain-based innovations including systems for managing intellectual property or safeguarding medical data, thereby satisfying legal criteria of novelty and non-observability.

Particularly in terms of personalized medicine and gene-editing technology, the United States provides more robust defenses for biotech patents. But the emergence of artificial intelligence in biotechnology begs problems regarding the inventiveness of AI-driven ideas, much as India's problems. With continuous debates on changing patent laws to fit AI-generated ideas, the U.S. legal system is more suited to handle these conflicts though. Unlike India, where the use of blockchain in patent applications is unclear, U.S. patent law is already changing to acknowledge blockchain's use in confirming patent claims and guaranteeing ownership transparency in biotechnological developments.

CYBERSECURITY CONCERNS IN BIOTECHNOLOGY SECTOR

Since blockchain technologies and artificial intelligence are being included into biotechnology more and more, protecting private information becomes crucial. Cybersecurity is controlled in India by the Information Technology Act of 2000 and its later revisions meant to guard against online dangers. Still vulnerable to advanced cyberattacks, the biotechnology industry handles enormous volumes of personal, genetic, and clinical data. Combining artificial intelligence with blockchain adds even more levels of complexity since both technologies may entail distributed networks appealing to cybercriminals and huge datasets.

India's legal system is continually developing to fit these demands. Although the Personal Data Protection Bill, 2019 aims to control personal data collecting, storage, and transfer, its relevance on the biotechnology industry is yet unknown. This begs questions about India's capacity to safeguard private biotechnology data, especially in relation to important uses like genetic research or medication development where artificial intelligence and blockchain are employed in vital capacity. In a world where data breaches and intellectual property theft are more common, the absence of industry-specific cybersecurity rules exposes Indian biotechnology firms to great hazards.

With regard to cybersecurity in biotechnology, the US views matters holistically. Along with additional industry-specific requirements, the Health Insurance Portability and Accountability Act (HIPAA) and the Cybersecurity Information Sharing Act of 2015 establish a good framework for safeguarding private biological and medical information. Artificial intelligence and blockchain are especially being used more and more in the biotech industry to enhance cybersecurity especially in safeguarding patient data and ensuring the integrity of clinical trial findings.

In the United States, where blockchain is being used to safely manage intellectual property, patient information, and genomic data, its importance in guaranteeing data security is especially remarkable. Blockchain lowers the possibility of data corruption and illegal access by decentralizing and encrypting data, so it is a perfect way to safeguard biotechnological resources. Furthermore, the U.S. government aggressively works with businesses to create cybersecurity rules addressing the particular difficulties presented by artificial intelligence and blockchain in biotech. This cooperative approach guarantees that the biotechnology industry stays strong against new cyber hazards and promotes creativity in AI-driven biotech solutions at the same time.

LEGAL AND ETHICAL IMPLICATIONS OF AI AND BLOCKCHAIN IN BIOTECHNOLOGY

Particularly in India, the integration of artificial intelligence and blockchain with biotechnology also begs serious ethical questions. Policymakers and stakeholders have engaged in discussions over data privacy, genetic information ownership, and artificial intelligence application in decision-making procedures. Lack of a thorough legislative structure controlling artificial intelligence and blockchain in biotechnology in India aggravates these moral conundrums. For example, if improperly controlled, the use of artificial intelligence to examine genetic data could result in privacy invasions. Likewise, the immutable character of blockchain begs questions regarding the storage and access to sensitive genetic data.

The ethical difficulties are further complicated by India's varied socioeconomic scene, where access to biotechnological advancements and the safeguarding of personal data may vary greatly among several spheres of society. Though more thorough laws are required to guarantee that AI and blockchain are utilized ethically in the biotechnology sector, the government's attempts to address these issues—such as through the enactment of the Personal Data Protection Bill—show great direction.

Similar ethical questions surround the United States, especially with relation to the use of artificial intelligence in medical decision-making and blockchain platform storage of genetic data. With organizations like the Food and Drug Administration (FDA) and the Federal Trade Commission (FTC) offering rules on the ethical use of artificial intelligence and blockchain in healthcare and biotechnology, the United States has a more established framework for handling these ethical concerns, nevertheless.

In the United States, artificial intelligence's involvement in biotechnology is considered as a two-edged blade: although it presents great possibility for developments in customized medicine and drug discovery, it also begs issues about responsibility, bias in AI algorithms, and possible use of genetic data. Although blockchain offers improved security, its permanent storing of private data raises moral questions. American policymakers are striving to strike a balance between ethical issues and innovation, therefore guaranteeing responsible application of blockchain and artificial intelligence in the biotechnology sector.

REGULATORY APPROACHES TO AI AND BLOCKCHAIN IN BIOTECHNOLOGY

Regulating systems in India regarding the integration of blockchain and artificial intelligence in biotechnology are still in their early years. Although the government has started conversations about artificial intelligence and new technologies, no particular legislation addresses their use in biotechnology. More general policies like the National Digital Health Blueprint and the draft National Strategy for Artificial Intelligence (AI), which encourage the use of AI across industries including healthcare and biotechnology, now shape the regulatory approach in India. These models are broad in nature, though, and they do not offer particular direction for the biotechnology sector or for blockchain-based projects in this field. Under the Department of Biotechnology, the Biotechnology Industry Research Assistance Council (BIRAC) helps to foster innovation in biotechnology—including digital technologies. India's biotechnology laws, however, mostly concentrate on conventional biotechnological innovations and pay scant to no attention to the legal subtleties brought up by artificial intelligence and blockchain. For biotech firms investigating the use of these technologies, especially in connection to intellectual property protection, data privacy, and cybersecurity standard compliance, this regulatory gap leaves ambiguity.

By contrast, the US has gone more forcefully to regulate artificial intelligence in biotechnology and blockchain. The Food and Drug Administration (FDA) has greatly helped to build a legislative framework for AI-driven medical devices, diagnostics, and other biotechnological applications. The FDA's Digital Health Innovation Action Plan outlines how artificial intelligence technologies could be introduced into medical equipment such that they meet safety and efficacy criteria. The FDA is also developing rules limiting the use of artificial intelligence in clinical research, personalized medicine,

and medication development. Particularly in connection to safeguarding consumers and maintaining data security in biotechnology, the U.S. Federal Trade Commission (FTC) has started studying how blockchain could be governed. Though blockchain itself is not especially controlled in the United States, its applications in sectors such biotechnology and healthcare are under close scrutiny to ensure adherence to present data security guidelines including HIPAA. The proactive regulatory approach applied in the United States provides biotechnology companies with a clearer legal path to employ artificial intelligence and blockchain technologies, therefore encouraging innovation even under regulatory control.

CHALLENGES IN HARMONIZING PATENT LAWS AND CYBERSECURITY STANDARDS

Harmonization of Patent Laws

The lack of uniformity among patent rules across different countries presents one of the main obstacles in including blockchain and artificial intelligence in biotechnology. Though both big participants in the biotechnology industry, India and the USA approach patenting biotechnological advances rather differently, particularly considering artificial intelligence and blockchain technologies. The patent system in India is more limited, with severe rules that can ban ideas or improvements involving human DNA or those too close to current technologies. This presents difficulties for biotechnology firms hoping to patent AI-driven inventions including perhaps little enhancements to currently used technologies. Conversely, although more flexible, the U.S. patent system presents certain difficulties with the advent of artificial intelligence. Both nations still have unsolved issues about inventorship—that is, whether an artificial intelligence system qualifies as an inventor. Still, the U.S. has been faster to modify its legal system to handle these problems; ongoing debates regarding changing patent rules to honor AI-generated innovations indicate Operating in both countries, biotechnology firms find it challenging to properly negotiate the patent terrain since patent rules lack international harmony.

Cybersecurity Standardization Challenges

Standardizing cybersecurity in biotechnology similarly presents a difficult task. Although blockchain offers a strong way to protect private biological data, its application is subject to different legal restrictions depending on India and the United States. Cybersecurity rules in India are scattered and lack clear laws controlling blockchain use in bioscience data security. Although these rules provide some degree of security, they are not fit for the complexity brought forth by artificial intelligence and blockchain in biotechnology. The Information Technology Act and the Personal Data security Bill.

Though the legal environment is better developed in the USA, there are currently no global guidelines for cybersecurity in biotechnology, especially when artificial intelligence and blockchain technologies are involved. Though these are not industry-specific, the National Institute of Standards and Technology (NIST) has developed recommendations for blockchain uses. For biotechnology firms, the lack of consistent cybersecurity systems across nations represents major hazards since they must negotiate a convoluted web of local rules to guarantee compliance.

Impact on Innovation and Collaboration in Biotechnology

In India, the regulatory uncertainties around artificial intelligence and blockchain in biotechnology could hinder innovation since businesses are reluctant to spend in technologies without clear legal protections. Lack of clarity in patent laws and lack of particular cybersecurity rules create obstacles for biotech companies wishing to investigate AI-driven research or blockchain for data security. Still, projects like BIRAC and the government's drive toward digital health via the National Health Stack offer some hope for the direction biotechnology research in India will go. These projects promote cooperation between the public and commercial sectors, therefore creating an atmosphere in which blockchain and artificial intelligence might be more important in furthering biotechnology development.

India's biotechnology industry might thus find it difficult to keep up with more developed countries like the USA, where artificial intelligence and blockchain are more easily included into biotech innovation processes, without more solid legal frameworks and clearer rules on intellectual property and data security.

Blockchain and artificial intelligence used in biotechnology are already generating notable innovation in the United States. The existing regulatory systems, especially those set by the FDA and USPTO, create a suitable environment for biotech firms to test novel technology. While blockchain is enhancing patient data security and openness of intellectual property management, artificial intelligence is accelerating medication research and optimizing clinical trials. By means of a cooperative strategy between regulatory authorities and commercial enterprises, breakthroughs in artificial intelligence and blockchain can be applied in biotechnology without endangering data security or safety. Furthermore, the American government's long-term dedication to promote innovation in biotechnology is shown by its expenditure in artificial intelligence research and development under programs like the National AI Initiative Act of 2020. For biotech firms wishing to investigate artificial intelligence and blockchain technologies, the United States offers clear legislative rules and strong intellectual property protection that appeal.

FUTURE DIRECTIONS FOR PATENT LAW AND CYBERSECURITY IN BIOTECHNOLOGY

India needs major changes in patent law and cybersecurity if it is to properly exploit artificial intelligence and blockchain in biotechnology. The Indian government has to provide a better legal framework addressing the particular difficulties presented by blockchain-based intellectual property management and AI-driven technologies. This includes going over the biotechnology patentability standards once more and thinking about changes acknowledging artificial intelligence as a possible innovator. India also has to create more tailored cybersecurity rules for the biotechnology industry to guarantee sufficient protection of private information created by AI systems or kept on blockchain platforms.

Regarding patent law and cybersecurity in biotechnology, United States prospects seem bright. Constant debates on artificial intelligence-generated inventions and the function of blockchain in intellectual property management imply that the United States is ready to modify its legal system to fit these

developing technologies. Ensuring that innovation in artificial intelligence and blockchain does not outstrip the legal protections in place will depend critically on ongoing cooperation between regulatory authorities and private corporations. Furthermore, as blockchain technology and artificial intelligence develop, the U.S. will have to modify its cybersecurity rules to fit the growing complexity of protecting biological data.

CONCLUSION AND RECOMMENDATIONS

In biotechnology, the combination of artificial intelligence with blockchain technology signals a turning point with great possibilities as well as considerable difficulties, particularly with relation to patent law and cybersecurity. Applied in biotechnology, these technologies present chances to transform fields including data security, genetic research, and medicine development. But the advent of these technologies also brings complex legal and regulatory questions, especially in nations like India and the United States where the approaches to patent law and cybersecurity vary in major respects.

Though in many respects thorough, India's present patent rules are not yet sufficiently flexible to allow for the explosive speed of development in artificial intelligence and blockchain technology. The legal system presents significant obstacles for biotechnology entrepreneurs since it does not provide clear instructions on patenting AI-generated inventions or blockchain management of intellectual property. Likewise, although gradually improving, India's cybersecurity system is still broad in scope and does not particularly handle the special difficulties presented by technologies like blockchain, especially in protecting sensitive biological data. India has to drastically change its patent laws and cybersecurity rules if it is to properly use artificial intelligence and blockchain in biotechnology. This would provide more legal certainty for inventors and guarantee strong protection of private data.

Conversely, the United States has a better developed legislative framework that fosters innovation in artificial intelligence and blockchain while also providing stronger intellectual property protection and a more sophisticated cybersecurity system. Blockchain's protection of private data, particularly in biotechnology, is already being acknowledged; the U.S. patent system is more adapted to manage the complexity provided by AI-generated inventions. But as both blockchain and artificial intelligence develop, the United States has to be alert, changing its cybersecurity rules and structures to foresee new risks especially as these technologies get more entwined into biology.

The road forward for India is a set of important actions to establish an environment fit for the merging of blockchain and artificial intelligence with biotechnology. First, changing the Patents Act to specifically target discoveries created by artificial intelligence and offer clearer rules on blockchain-based technologies will help to lower legal uncertainty. This will help biotech innovators negotiate the patent system more effectively, therefore guaranteeing that their creations are sufficiently covered by the law. Given the sensitive nature of data in the biotechnology industry particularly, India also has to create a more customized cybersecurity legislative framework unique to this industry. By ensuring that such rules complement international best practices, Indian biotech enterprises will be able to run safely on a worldwide level. Moreover, the government should support public-private cooperation—like those developed by BIRAC—to inspire cooperation between businesses and regulatory authorities. This kind

of cooperation can promote biotechnology research and help solve technical and legal issues presented by these developing technologies.

The United States depends on ongoing improvement of patent rules to solve particular problems raised by artificial intelligence-driven innovations. More precise definitions of inventorship—especially in circumstances when artificial intelligence is heavily involved—are required to guarantee that the U.S. patent system stays adaptable and equipped to safeguard cutting-edge biotechnological developments. Moreover, resolving the cybersecurity concerns resulting from the growing integration of artificial intelligence and blockchain in biotechnology would depend mostly on cooperation between regulatory authorities and commercial enterprises. Especially in relation to blockchain, the U.S. should also concentrate on keeping ahead of these hazards by funding research and development targeted at safeguarding private biological data. At last, international cooperation on harmonising cybersecurity rules and patent laws would assist to ease the legal complexity experienced by biotechnology firms running across several countries. Such initiatives will help to streamline innovation processes, so allowing the full possibilities of artificial intelligence and blockchain to be realised all around.

With blockchain and artificial intelligence helping biotechnology to develop, the need of strong patent and cybersecurity systems becomes more urgent. Although both India and the United States have strong roles in the worldwide biotechnology sector, their legal and regulatory systems are quite different. India faces the difficulty of implementing significant changes to remain competitive on the international scene, while the United States has been more aggressive in adjusting its regulatory structure to help the incorporation of modern technology.

The intersection of artificial intelligence, blockchain, and law will probably help to define biotechnology going forward. The difficulty for both India and the United States is building legal systems that not only safeguard intellectual property and guarantee data security but also actively support invention. Important actions for both nations will be addressing the legal ambiguities of artificial intelligence-generated inventions and blockchain-based intellectual property management as well as improving cybersecurity standards. By implementing these steps, India and the United States may establish themselves as leaders in the biotechnology revolution, therefore promoting major developments that will shape medicine and healthcare going forward.

*****

BIBLIOGRAPHY

1. U.S. Pat. & Trademark Off., Patentable Subject Matter—Living Subject Matter, 1999 (Apr. 1, 1999), https://www.uspto.gov/web/offices/pac/mpep/mpep-9025.html.
2. Nat'l Inst. of Standards & Tech., Blockchain Technology Overview (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

3. Dep't of Biotech., Gov't of India, Biotechnology Industry Research Assistance Council (BIRAC), https://www.birac.nic.in/.
4. Food & Drug Admin., Digital Health Innovation Action Plan (2017), https://www.fda.gov/media/106331/download.
5. The Patents Act, No. 39 of 1970, India Code (1970).
6. Draft National Strategy for Artificial Intelligence, AI for All, NITI Aayog (2018), https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
7. Nat'l Comm'n for the Protection of Human Subjects of Biomedical & Behavioral Research, The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research (1979), https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.
8. Information Technology Act, No. 21 of 2000, India Code (2000).
9. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936.
10. Michael A. Carrier, Blockchain and Intellectual Property Law: A Case for Transparency in Patent Ownership, 21 STAN. TECH. L. REV. 139 (2018).
11. Jennifer Doudna & Emmanuelle Charpentier, CRISPR-Cas9 and the Future of Biotechnology, 53 AM. J. BIOTECH 15 (2017).
12. National AI Initiative Act of 2020, Pub. L. No. 116-283, 134 Stat. 3388.
13. R. Dreyfuss, Artificial Intelligence and the Role of Law in Biotechnology Patents, 17 HARV. J. L. & TECH. 1 (2003).

******

NAVIGATING THE ETHICAL LANDSCAPE: ARTIFICIAL INTELLIGENCE IN CHILD WELFARE SYSTEMS

Apoorwa Pandey[32] and Subha[33]

ABSTRACT

Artificial intelligence (AI) presents important ethical challenges as well as exciting prospects for child welfare systems that employ AI. The delicate field of child protection services and the intricate interactions amongst AI technologies will be investigated in this paper. Even while AI has the ability to improve decision-making, early threat detection, and utilization of resources, there are serious ethical issues with its application. These include concerns about data bias, privacy, transparency, and the possibility that AI could contribute to already-existing structural injustices. The study investigates how the use of artificial learning and predictive analytics in child welfare situations may unintentionally reinforce biased behaviours or result in unnecessary interventions. It also discusses the moral ramifications of data collecting and storage, taking into account the long-term effects on families and kids whose private data is used by artificial intelligence (AI) algorithms. The topic of debate also includes the difficulty of upholding human judgment and empathy in a field where a complex grasp of interpersonal relationships is essential. The study makes the case for a sensible strategy that prioritizes ethical issues and children's welfare while utilizing AI's strengths. It ends by outlining a framework for the responsible application of AI in child welfare, highlighting the necessity of continuing ethical assessment, stakeholder involvement, and adaptive governance to guarantee that AI adds to the skills of humans in safeguarding susceptible youngsters rather than taking their place.

Keywords: Artificial Intelligence, Child Welfare, Ethical Implications, Predictive Analytics, Data Privacy

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) has brought about transformative changes across various sectors, with particularly significant implications for child welfare systems and cybersecurity. This intersection represents a critical area of study, as organizations responsible for protecting vulnerable children increasingly rely on digital systems to manage sensitive information and deliver essential services. The integration of AI in child welfare systems promises enhanced efficiency, improved decision-making, and better outcomes for children and families. However, this digital transformation also introduces new cybersecurity challenges that must be carefully managed.

To navigate these challenges successfully, organizations must adopt best practices across technical, organizational, and ethical domains. Technical best practices should focus on ensuring system reliability and security through robust architecture and regular updates. Organizations should implement comprehensive testing procedures to validate AI system performance while also establishing backup and recovery protocols. Organizational best practices emphasize the importance of human elements in AI implementation. Comprehensive training programs are necessary to prepare staff at all levels to work effectively with AI systems while clear policies should guide system use and decision-making processes. Regular evaluations will help organizations adapt their strategies to changing needs. Ethical guidelines provide the foundation for responsible AI implementation. Organizations must maintain

[32] Research Scholar at Dr. C.V. Raman University, Kota.
[33] Research Scholar at Bharti Vishwavidyalaya, Durg (C.G.), India.

transparency in decision-making processes while establishing accountability mechanisms for their actions related to children's rights principles. Regular ethical assessments will help ensure alignment with organizational values while addressing emerging challenges. In conclusion, this study aims to provide a comprehensive analysis of current practices, challenges, and opportunities while offering actionable recommendations for organizations seeking to leverage AI technologies effectively. By following established best practices while prioritizing ethical guidelines throughout all implementations, organizations can harness the potential offered by this technology responsibly—protecting vulnerable populations while ensuring robust security measures are maintained as we move forward into an era defined by rapid technological change.

AI APPLICATIONS IN CHILD WELFARE SYSTEMS

The integration of AI in child welfare systems has fundamentally transformed traditional approaches to child protection and family support services. These applications span multiple areas of operation, from risk assessment to case management and resource allocation, creating a more efficient and effective system for protecting vulnerable children.

One of the most promising applications of AI in child welfare is predictive analytics for risk assessment. These sophisticated systems analyse vast amounts of historical data to identify patterns and risk factors that might not be immediately apparent to human caseworkers. By processing information from multiple sources including case histories, demographic data, and service utilization patterns AI algorithms can flag high-risk cases before they escalate into crisis situations. This predictive capability enables child welfare agencies to allocate resources more effectively and intervene proactively rather than reactively.

Moreover, the enhancement of case management through AI has revolutionized how child welfare professionals handle their daily responsibilities. Automated documentation and report generation systems significantly reduce the administrative burden on caseworkers, allowing them to spend more time directly supporting families. AI-powered systems can intelligently match services with family needs, optimize workload distribution among staff, and provide real-time monitoring of case progression. This integration creates a comprehensive view of each case, enabling informed decision-making and better outcomes for children and families.

Early intervention strategies have also been significantly strengthened through AI applications. These systems can identify at-risk families before crisis situations develop, enabling targeted prevention programs based on community needs. The automated screening of referrals helps agencies process information more quickly and accurately while continuous monitoring ensures that resources are used optimally. This proactive approach has shown promising results in reducing the incidence of serious child welfare cases and improving family outcomes.

THE DUAL NATURE OF AI IN CYBERSECURITY

The implementation of AI in cybersecurity presents both remarkable protective capabilities and significant vulnerability concerns, creating a complex dynamic that organizations must carefully

navigate. This dual nature is particularly relevant in child welfare systems, where the protection of sensitive information is paramount.

On the protective side, AI strengthens cybersecurity through advanced threat detection using machine learning algorithms. These systems can monitor network traffic in real-time, identifying and responding to potential security incidents before they cause significant damage. Pattern recognition capabilities allow AI systems to detect unusual behaviour that might indicate a security breach while automated security updates help maintain system integrity. The predictive analysis of potential security threats enables organizations to stay ahead of emerging cybersecurity challenges.

However, the integration of AI systems also introduces new vulnerabilities that must be carefully managed. Malicious actors may attempt to exploit AI algorithms through various attack vectors, including model manipulation and adversarial attacks. The extensive data collection required for AI systems raises privacy concerns, particularly regarding the storage and protection of sensitive information about children and families. Organizations must also address the challenge of maintaining AI system integrity while ensuring these systems remain accessible to authorized users.

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN CHILD WELFARE SYSTEMS: A GLOBAL PERSPECTIVE

United States

Implementation Areas:

1. Predictive Analytics Systems
2. Allegheny County (Pennsylvania) - Allegheny Family Screening Tool (AFST)
3. Illinois - DCFS Predictive Analytics Initiative
4. Florida - Child Welfare Early Warning System

Key Features:

- Risk assessment and prediction of child abuse/neglect
- Resource allocation optimization
- Case prioritization
- Family support service matching

Australia

Implementation Areas:

1. Decision Support Systems
2. Child Protection Information System
3. Family Support Network Analytics

Key Features:

- Early intervention identification

- Cross-agency data sharing
- Automated reporting systems
- Risk pattern identification

New Zealand

Implementation Areas:

1. Integrated Data Infrastructure
2. Predictive Risk Modeling (PRM)
3. Social Investment Analytics Layer

Key Features:

- Population-level risk assessment
- Service effectiveness evaluation
- Resource allocation optimization
- Preventive intervention planning

United Kingdom

Implementation Areas:

1. Child Protection Information Sharing System
2. Multi-agency data sharing platforms
3. Early Help Module

Key Features:

- Cross-border information sharing
- Real-time alert systems
- Case management automation
- Risk factor analysis

The implementation of AI in child welfare systems varies significantly across countries, with different approaches and levels of sophistication. While some nations focus on predictive analytics and risk assessment, others emphasize case management and service delivery optimization. The success of these implementations depends heavily on careful consideration of technical, operational, and ethical challenges, along with adherence to best practices and continuous evaluation of outcomes.

ETHICAL CONSIDERATIONS IN AI IMPLEMENTATION

The implementation of AI in child welfare systems raises significant ethical considerations that must be balanced against the potential benefits. Privacy and data protection are fundamental concerns in AI-enabled child welfare systems. Organizations must establish robust frameworks for safeguarding sensitive personal information while ensuring appropriate data collection practices. The management

of consent becomes increasingly complex in digital systems, requiring careful attention to both legal requirements and ethical considerations. Long-term privacy interests of children must be protected, recognizing that information collected today may have implications far into the future.

Algorithmic bias presents another ethical challenge in AI-enabled child welfare systems. There is a critical need to address potential discrimination in automated decision-making processes, particularly regarding racial, ethnic, and socioeconomic factors. Organizations must implement regular bias assessments while maintaining transparency in how AI systems make recommendations. This includes developing comprehensive fairness metrics and monitoring systems to ensure equitable treatment across all demographic groups.

The implementation of AI in child welfare systems must prioritize the children's rights framework, ensuring that while AI enhances service delivery and decision-making, it does not compromise children's fundamental rights to participation, privacy, and appropriate care. This framework is essential because it reinforces the idea that children are not just passive recipients of services but active participants in decisions that affect their lives. As organizations leverage AI technologies to improve outcomes, they must also ensure that these technologies do not undermine the rights of children. For instance, AI systems should be designed to facilitate children's voices in decision-making processes, allowing them to express their needs and preferences effectively. This approach fosters a sense of agency among children and helps create a more child-cantered welfare system.

In India, the legal framework surrounding children's rights is robust, with various laws and policies aimed at protecting and promoting the rights of children. The Constitution of India provides for fundamental rights that include the right to equality, the right to freedom from discrimination, and the right to protection from exploitation. Additionally, the Juvenile Justice (Care and Protection of Children) Act, 2015 emphasizes the need for child welfare systems to prioritize the best interests of the child. This legal context becomes particularly relevant when integrating AI into child welfare systems. Organizations must ensure that AI applications align with these legal provisions, safeguarding children's rights while utilizing technology for better service delivery. The National Policy for Children (2013) further reinforces this commitment by recognizing children as a vulnerable group deserving special attention and protection.

While AI can significantly enhance child welfare services by improving efficiency and effectiveness, organizations must strike a delicate balance between leveraging these capabilities and maintaining meaningful human oversight in decisions affecting children's lives. Human oversight is critical in ensuring that AI-generated recommendations are interpreted within the broader context of each child's unique circumstances. It is essential for practitioners to remain involved in decision-making processes, particularly when it comes to sensitive issues such as child protection and family support. This oversight helps mitigate potential biases inherent in AI algorithms and ensures that decisions are made with empathy and understanding. Moreover, organizations should implement mechanisms for accountability and transparency in AI use, allowing stakeholders—including families and children—to understand how decisions are made and to challenge them if necessary.

In conclusion, as child welfare organizations increasingly adopt AI technologies, they must remain vigilant in upholding children's rights throughout this process. By embedding a strong children's rights framework into their operations, aligning with India's legal standards, and ensuring human oversight in decision-making, organizations can harness the potential of AI responsibly. This approach will not only enhance service delivery but also protect vulnerable populations from potential harms associated with technology misuse. Ultimately, integrating AI into child welfare systems offers an opportunity to create a more responsive and inclusive environment for children and families while safeguarding their fundamental rights.

CHALLENGES AND BEST PRACTICES FOR IMPLEMENTATION

The implementation of AI in child welfare systems faces numerous technical, organizational, and policy-related challenges that must be addressed carefully to ensure successful outcomes. Technical challenges represent significant hurdles in AI implementation; many child welfare organizations struggle with legacy systems that are difficult to integrate with modern AI solutions. Data quality issues can impact the effectiveness of algorithms while infrastructure requirements may strain organizational resources.

Organizational challenges often prove equally daunting. The introduction of AI systems requires substantial change management efforts to overcome resistance among staff who must learn to utilize new technologies effectively while maintaining their focus on family support. Resource allocation decisions become more complex as organizations balance technology investments with other critical needs.

Policy-related challenges create another layer of complexity; organizations must navigate varying compliance requirements across jurisdictions while adapting to evolving legal frameworks governing AI use in social services. The development of appropriate standards for AI implementation in child welfare requires careful consideration of both technical and ethical factors.

Successful implementation requires adherence to established best practices across technical, organizational, and ethical domains. Technical best practices focus on ensuring system reliability and security; organizations should implement robust security architecture with regular updates while establishing comprehensive testing procedures to validate system performance.

Organizational best practices emphasize the human elements of AI implementation; comprehensive training programs should prepare staff at all levels to work effectively with AI systems while clear policies guide system use. Ethical guidelines provide the foundation for responsible AI implementation; organizations must maintain transparency in decision-making processes while establishing accountability mechanisms for their actions related to children's rights principles.

FUTURE DIRECTIONS

The future holds both promising opportunities and significant challenges that organizations must prepare to address as emerging technologies expand possibilities for AI applications in child welfare.

Advanced machine learning algorithms offer increasingly sophisticated predictive capabilities while improvements in natural language processing enhance system accessibility.

Policy development must keep pace with technological advancements by addressing both opportunities and risks associated with AI implementation. International cooperation becomes increasingly important as child welfare cases cross jurisdictional boundaries; developing standards requires ongoing collaboration between technology experts, child welfare professionals, and policymakers.

Research priorities should focus on long-term impact assessments of AI implementations in child welfare systems; studies must examine both the effectiveness of interventions enabled by AI as well as their implications for children's rights and well-being.

In conclusion, the integration of AI into child welfare systems represents a significant advancement but requires careful attention to both opportunities and challenges associated with its use. Organizations must balance potential benefits with robust security measures and ethical practices by developing comprehensive governance frameworks addressing both technical considerations as well as ethical guidelines.

By following established best practices while prioritizing ethical guidelines throughout all implementations organizations can harness the potential offered by this technology responsibly protecting vulnerable populations while ensuring robust security measures are maintained as we move forward into an era defined by rapid technological change.

*****

REFERENCES

1. R. Alfandari, "Algorithmic decision-making in child protection: Human rights issues", International Human Rights Law Review, vol. 8, no. 2, pp. 201-228, 2019.
2. A. Brown, A. Chouldechova, E. Putnam-Hornstein, A. Tobin, and R. Vaithianathan, "Toward algorithmic accountability in public services: A qualitative study of affected community perspectives on algorithmic decision-making in child welfare services", in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1-12, 2019.
3. R. Carrillo and M.A. Curran, "Artificial intelligence in child welfare: Considerations for responsible implementation", Children and Youth Services Review, vol. 121, p. 105885, 2021.
4. S. Cuccaro-Alamin, R. Foust, R. Vaithianathan, and E. Putnam-Hornstein, "Risk assessment and decision making in child protective services: Predictive risk modeling in context", Children and Youth Services Review, vol. 79, pp. 291-298, 2017.
5. M. De-Arteaga, R. Fogliato, and A. Chouldechova, "A case for humans-in-the-loop: Decisions in the presence of erroneous algorithmic scores", in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-12, 2020.
6. V. Eubanks, Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018.

7. M. Haar, F.J. van de Vijver, and A. Broeders, “Human rights implications of algorithmic decision-making: A review of the literature”, International Journal of Human Rights, vol. 25, no. 6, pp. 1-21, 2021.
8. Illinois Journal of Law Technology & Policy, “Harnessing AI innovation for struggling families”, Available at: https://illinoisjltp.com/journal-archive/volume/null/article/harnessing-ai-innovation-for-struggling-families-1 [Accessed 24 Oct. 2024].
9. Imprint News, “Using algorithms & artificial intelligence in child welfare”, Available at: https://imprintnews.org/child-welfare-2/using-algorithms-artificial-intelligence-in-child-welfare/33429 [Accessed 24 Oct. 2024].
10. Imprint News, “Child welfare should go slow on AI: A cautious approach to technology integration in sensitive areas of social work practice”, 2024. Available at: https://imprintnews.org/opinion/child-welfare-should-go-slow-ai/242819 [Accessed 24 Oct. 2024].
11. D. Leslie, L. Holmes, C. Hitrova, and E. Ott, Ethics and governance of artificial intelligence for health. World Health Organization, 2020.
12. OAL Law, “The transformative power of AI in the growing cybersecurity threats and cyber-attacks”, Available at: https://oal.law/the-dual-nature-of-artificial-intelligence-ai-transformative-power-of-ai-in-the-growing-cybersecurity-threats-and-cyber-attacks/ [Accessed 24 Oct. 2024].
13. Rainbow Secure, “The dual nature of artificial intelligence (AI) in cybersecurity”, Available at: https://www.linkedin.com/pulse/dual-nature-artificial-intelligence-ai-cybersecurity-rainbowsecure/ [Accessed 24 Oct. 2024].
14. ResearchGate, “Improving human-AI partnerships in child welfare: Understanding worker practices, challenges, and desires for algorithmic decision support”, Available at: https://www.researchgate.net/publication/360250082 [Accessed 24 Oct. 2024].
15. N.A. Saxena, K. Huang, E. DeFilippis, G. Radanovic, D.C. Parkes, and Y. Liu, “How do fairness definitions fare? Examining public attitudes towards algorithmic definitions of fairness”, in Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, pp. 99-106, 2019.
16. I.M. Schwartz, P. York, E. Nowakowski-Sims, and A. Ramos-Hernandez, “Predictive and prescriptive analytics, machine learning and child welfare risk assessment: The Broward County experience”, Children and Youth Services Review, vol. 81, pp. 309-320, 2017.
17. Social Work Podcast, “ChatGPT4o: Exploring AI's role in social work practice”, 2024. Available at: https://socialworkpodcast.blogspot.com/2024/05/ChatGPT4o.html [Accessed 24 Oct. 2024].

18. Unisys, “8 ways AI and ML are transforming child welfare”, Available at: https://www.unisys.com/blog-post/cis/8-ways-ai-and-ml-are-transforming-child-welfare/ [Accessed 24 Oct. 2024].
19. R. Vaithianathan, E. Putnam-Hornstein, N. Jiang, P. Nand, and T. Maloney, “Developing predictive models to support child maltreatment hotline screening decisions: Allegheny County methodology and implementation”, Centre for Social Data Analytics, 2017.
20. World Economic Forum, “AI governance: A holistic approach to implement ethics into AI”, World Economic Forum White Paper, 2020.

*****

AI-ENACTED CYBERSECURITY: STRENGTHNING DEFENCES AGAINST CYBERCRIMES

Madireddy Divitha Reddy[34]

ABSTRACT

Artificial intelligence (AI) is transforming cybersecurity by delivering enhanced capabilities for defending against ever developing cyber threats. As fraudsters develop advanced strategies, enterprises must use AI-powered solutions to remain ahead. AI has the ability to handle massive volumes of data at unprecedented speeds, allowing cybersecurity systems to evaluate large-scale data sets created by network traffic, user activity, and system logs to detect possible threats. Traditional methods do not succeed to handle the massive amount and depth of this data, leading to delay or missing threat detection. Machine learning (ML), a kind of artificial intelligence, is particularly capable of identifying earlier unidentified threats, sometimes referred to as zero-day attacks. Traditional signatures solutions, like antiviral software, rely on databases that contain known risks and have no ability to identify new, sophisticated attacks. The ability of artificial intelligence to learn from previously collected information helps it to identify unforeseen trends in the network's communications or user actions that might indicate an approaching risk, giving another level of protection.AI improves the automation of threat identification and incident response. As cyberattacks become more frequent and complicated; it's manually reacting to every single alert or the case can overload cybersecurity workforce. Systems powered by AI can categorize risks based to their level of seriousness, enabling teams to focus on the most significant issues. Artificial intelligence (AI) technology may also respond automatically to certain forms of attacks like disconnecting compromised devices or blocking suspected communication. But the use of artificial intelligence in cybersecurity faces obstacles. A major problem is the rise of competition AI, which allows attackers to create more complex attacks. With these drawbacks, the application of artificial intelligence in cybersecurity has grown more essential. The use of AI into cybersecurity strategies provides an opportunity to offer quicker, flexible, and affordable security ways. As cyber-attacks grow, AI is going to have a more significant part in improving industries' defences, decreasing response times, and providing better security against an increasing variety of cybercrimes.

Keywords: Artificial Intelligence, Cyber-attacks, Cybersecurity, Machine Learning, Traditional signatures solutions.

INTRODUCTION

As the digital world becomes increasingly linked, cybercrime has emerged as one of the most serious risks to individuals, corporations, and governments. Cybercrime is now an important problem, with worldwide damages projected to exceed $10.5 trillion per year by 2025. Cybercriminals use cutting-edge technology and world-wide networks to attack flaws in anything from personal electronic devices to big corporate infrastructures. This increasing risk requires better and more flexible safety measures that go beyond standard approaches. Major industries, such as finance, health care, and the government, are particularly at risk, as financial institutions are frequently targeted for financial gain, and health care providers are valued for their personal information that is sensitive. Important infrastructures, such as power lines and transportation systems, face greater dangers of cyberattacks with serious impact on society. This complex and expanding threat landscape necessitates more advanced cybersecurity

[34] Student at Christ Academy Institute of Law, India.

solutions, as old systems become increasingly ineffective. Traditional cybersecurity methods have evolved to address some of these issues, but these advances are insufficient. Cybercriminals are frequently several steps ahead, needing a more proactive, intelligent response as Artificial Intelligence (AI) has an opportunity to transform cybersecurity by providing a more dynamic and predictable approach. Artificial intelligence (AI) is especially appropriate to cybersecurity as it specializes at analysing huge amounts of data, recognizing trends, and identifying defects in real time, each of which have become essential in fighting against cybercrime. Bad actors are also exploring generative AI's potential to aid cyberattacks through innovations such as self-evolving malware.

One of the most important aspects that artificial intelligence brings in cybersecurity is its capacity for continuous surveillance and detection of threats. AI-driven structures, without human's experts, are capable of monitoring connections for suspicious activity 24 hours a day, and seven days a week. These systems may continually acquire knowledge from historical as well as current information using artificial intelligence (ML), a subset of AI, recognizing new hazards before they do damage. AI may also dramatically cut reaction times.

As the thesis of the paper, AI-enacted security measures provide effective safeguards from the constantly evolving cybercrime scene, with creative ways to detect, cease, and reduce threats. The systems in question do, however, also present important ethical, data privacy, and governmental oversight problems that need to be resolved to guarantee their efficacy and security. The paper explores the way artificial intelligence (AI) can help with the field of cybersecurity, having a special focus on the way it might strengthen anti-cybercrime efforts. It looks at how artificial intelligence (AI) tools including automated threat detection, machine learning, and neural networks support stronger cybersecurity strategies. The benefits and drawbacks of AI-enacted cybersecurity systems are addressed as well in the paper. his enhancement to support data-processing may increase the efficiency of algorithms. Algorithms are key components of running AI and may be tailored to counter complex cyber threats. An algorithm is a set of step-by-step instructions given to a computer to accomplish a specific task. AI may push this technology to another level, to achieve intelligent autonomous algorithms. Artificial Intelligence will identify future dangers before they become actual because to its predictive skills, and it can work continuously to provide real-time security without continual human interaction. The rapid implementation of AI in cybersecurity, data privacy, and responsibility in the event of failure or misuse are some of the legal and moral concerns brought up by its implementation. The importance of thorough strategies which maintain a balance between innovation and civil rights are additionally highlighted in the study.

THE CYBERCRIMES LANDSCAPE

The worldwide cybercrime scene has grown exponentially, with hackers constantly changing and inventing their strategies. Hacking and attacks using social engineering, the threat of ransom spyware, viruses, sophisticated persistent threats (APTs), and weaknesses in the Internet of Things (IoT) are examples of common cybercrimes. Cybercrime has profound economic and societal consequences, with the World Economic Forum estimating that annual costs will exceed $10.5 trillion by 2025.With the increasing sophistication of hackers, traditional security precautions face significant problems.

Traditional cybersecurity depends heavily on interactions between people in order to recognize, evaluate, and react to dangers, which may be slow and prone to mistakes, especially while dealing with large-scale assaults or multiple risks at the same time. Signature-based detection approaches, which depend on established patterns of recognized threats, do not identify novel, unknown, or threats are developing. Cybercriminals often create malware with versatile properties, altering their code to avoid signature-driven security.

Static defences, like as firewalls or intrusion detection systems, are intended to defend networks from external attacks but are ineffective against novel, unknown, or developing dangers. Nowadays, cybercriminals constantly search for imperfections, enabling cyberattacks more flexible and dynamic. This calls for a similarly adaptable and responsive protective strategy, which can be hard to execute via traditional approaches. Security teams may experience alert fatigue as a result of the deluge of data and warnings produced by Security Information and Event Management (SIEM) systems. This can cause them to miss chances to address actual threats and slow down reaction times when events do occur. The dynamic and ever-changing nature of contemporary cyberthreats underscores the necessity of real-time threat detection and response capabilities. Conventional solutions that depend on human interaction and preset detection models are unable to address the ever-changing and dynamic nature of cybercrime. AI-powered cybersecurity solutions provide an answer to these problems. AI may examine data by using machine learning techniques analysing huge amounts of information in real time, identifying unexpected trends and patterns that may suggest the existence of a cyberthreat. It is not necessary to know the attack signatures in advance for these technologies to adjust to new threats.

ARTIFICIAL INTELLIGANCE IN CYBERSECURITY: TRANSFORMATIONAL POTENTIAL

Machine learning (ML) is an important AI technique that allows computers to learn from previously collected information, identify patterns, and recognize variations in real time. This is necessary to recognizing risks that conventional systems based on rules may neglect. Machine learning (ML) additionally finds application in analysis of behaviours, involving programs tracking and assessing user activities to find variations from typical conduct. In cybersecurity, MLis used to detect unusual behavior, classify threats, and adapt to new types of attacks. It improves threat intelligence by processing huge amounts of data from many sources to discover new threats. In order to identify and counter social engineering schemes and hacking assaults, the use of natural language processing, or NLP, is necessary. The algorithms used in NLP can identify patterns that indicate hacking efforts, such as suspicious URLs, which are deceitful language, and impersonation. Additionally, they may assess the setting and tone of interactions to avoid

This not only improves efficiency but also minimizes the time required to mitigate hazards. AI-enhanced systems have shown promise in detecting zero-day flaws by recognizing behavioural anomalies associated with the early phases of an assault. In 2021, for example, Darktrace successfully spotted and mitigated a zero-day vulnerability aimed at a multinational company's network. AI-powered systems have proven extraordinary success in avoiding data intrusions. IBM's Watson for Cyber Security thwarted to assaults using social engineering that try to Tinfluence how people behave. AI-

driven automation is changing the way security operation centres (SOCs) react to cyber assaults. By doing low-level, repetitive chores like patching security flaws, reacting to known threats, and scanning for vulnerabilities, automated systems free up human analysts to work on more difficult and important problems. This shortens the time needed to mitigate hazards in addition to increasing efficiency. AI-enhanced systems have demonstrated efficacy in finding zero-day vulnerabilities through the identification of behavioural abnormalities linked to the initial phases of an assault. In 2021, Darktrace, for instance, was able to locate and eliminate a zero-day attack that was aimed at the network of a global corporation. Data breaches have been successfully prevented by AI-powered technologies; IBM's Watson for Cyber Security stopped a major effort in 2020 to hack a financial institution's data. In the field of AI-Enhanced Ransomware Detection, AI has additionally demonstrated itself to be essential. Critical patient data was preserved in 2022 after CrowdStrike identified early warning signs of a ransomware assault on a healthcare institution.

STARNGTEHENING

The rapid digitization of economies, businesses, and personal data has created new opportunities but also exposed vulnerabilities to cybercriminals. As cyber threats continue to evolve, Artificial Intelligence (AI) emerges as a powerful ally in fortifying cybersecurity by offering dynamic, real-time solutions to predict, prevent, and respond to threats.

AI's most promising applications in cybersecurity include threat detection and prevention through big data analysis and predictive modelling. AI systems can analyse vast amounts of data from various sources, such as network traffic, social media, and dark web monitoring, to identify patterns, trends, and anomalies that could signify potential threats. By analysing these complex data points in real-time, AI-powered systems can give early warnings, allowing organizations to bolster their defenses before a breach occurs. AI-driven systems are also adept at identifying patterns across vast and complex networks, making them invaluable in spotting attempts at data exfiltration. When malicious actors try to siphon sensitive data, AI can track these activities across multiple endpoints and alert cybersecurity teams of the suspicious behavior. With AI's ability to process high volumes of data at incredible speeds, security teams are equipped with the insights needed to prevent attacks more effectively, reducing their dependency on human intervention.Real-time response and automation are another key feature of AI. In the event of a cyberattack, AI significantly reduces the window between detection and action, helping minimize damage. Traditional cybersecurity solutions often depend on manual response systems that can take hours, if not days, to react. In contrast, AI-powered systems work in real-time, automatically identifying and isolating threats as they emerge. This instantaneous response not only reduces the impact of attacks but can also prevent their spread across networks.

Automation is another key feature of AI, revolutionizing cybersecurity by automating repetitive tasks such as patch management and network monitoring. Cybersecurity teams are often overwhelmed with maintaining and updating security patches or monitoring network activity for signs of intrusions. AI can take over these tasks, ensuring that patches are applied promptly to eliminate vulnerabilities and network anomalies are continuously monitored without the need for constant human oversight. AI also enhances user authentication through innovative, AI-driven authentication systems like biometrics and

behaviour-based authentication. These systems analyse and verify physical traits such as fingerprints, facial recognition, or voice patterns, ensuring that only authorized users gain access to sensitive systems or data. By incorporating AI into cybersecurity strategies, organizations can stay one step ahead of attackers and safeguard their data and operations in an ever-changing cyber environment.

ETHICAL AND REGULATORY CHALLENGES

While the quick digitalization of corporations, economies, and personal data has opened up new possibilities, it has also made hackers more vulnerable. Artificial Intelligence (AI), which provides dynamic, real-time solutions to anticipate, avoid, and respond to attacks, is becoming a potent ally in bolstering cybersecurity as cyber threats continue to change. Big data analysis and predictive modeling are two of AI's most potential uses in cybersecurity for threat identification and prevention. AI systems are capable of analyzing enormous volumes of data from a variety of sources, including social media, network traffic, and dark web surveillance, in order to spot trends, patterns, and anomalies that can indicate possible dangers. AI-powered systems may provide early warnings by evaluating these intricate data points in real-time, enabling businesses to strengthen their defences before a breach happens. AI-powered systems are also skilled in finding patterns in large, intricate networks, which makes them important in spotting data exfiltration efforts. AI can monitor these actions across several endpoints and notify cybersecurity professionals of any questionable activity when malevolent actors attempt to steal confidential information. Security teams are less dependent on human involvement since AI can handle large amounts of data at amazing rates, giving them the insights they need to stop assaults more successfully. Transparency is another ethical challenge. AI systems, particularly those based on deep learning, can actus "black boxes," making decisions that are difficult for humans to understand or interpret. Another important aspect of AI is its ability to respond in real time and automate tasks. AI greatly shortens the time between discovery and response in the case of a cyberattack, assisting in minimizing damage.

FUTURE TRENDS AND CHALLLENGES

AI is transforming cybersecurity by improving the powers of detection, response, and prevention. A significant development, deep learning allows computers to recognize and learn from intricate patterns in large datasets, improving threat detection capabilities and more accurately differentiating between benign and malicious activity than conventional systems. By addressing the vulnerabilities brought about by the growth of Internet of Things (IoT) devices, artificial intelligence (AI) in IoT security lowers the chances of IoT security breaches. In cybersecurity, quantum computing offers both possibilities and difficulties. Although it has the potential to transform encryption techniques, quantum-enabled cyberattacks might make existing cryptographic safeguards outdated. One urgent issue is the race to create cryptography systems that are immune to quantum errors. But even while AI has the potential to improve cybersecurity, a number of obstacles prevent its broad application. One of the technical obstacles is the intricacy. difficulty incorporating AI into current cybersecurity frameworks, which may make it challenging to upgrade infrastructure without interfering with essential services. Furthermore, for AI to work efficiently, enormous volumes of data are needed, and maintaining the quality and integrity of this data is crucial to preventing missing risks or false positives. An arms race between

attackers and defenders is also brought about by the development of AI. AI is being used by cybercriminals to create increasingly complex assaults that are harder to stop. Federated learning and other collaborative AI systems present a viable way to combat worldwide, constantly changing cyberthreats. To create frameworks and standards for AI in cybersecurity that promote ethical usage and innovation, international cooperation is crucial.

CONCLUSION

AI-enhanced cybersecurity has various advantages, including quicker threat detection, real-time reactions, and stronger protection systems. Machine learning algorithms and predictive analytics enable AI systems to detect vulnerabilities and respond to emerging attacks, decreasing human error and enhancing overall security. AI's automation capabilities expedite operations ranging from intrusion detection to user authentication, offering a strong line of defence against sophisticated cyber threats. However, ethical and legal difficulties persist, including questions about data privacy, transparency, and accountability. The complexity of AI systems also raises concerns about abuse, prejudice, and over-reliance on automated decision-making. Ensuring ethical AI usage, protecting privacy, and developing clear legal frameworks are critical for avoiding these concerns. The future of AI-enacted cybersecurity has enormous promise, but reaching its full potential demands a balance between innovation and accountability. International cooperation, ethical tracking, and strong regulatory norms must all work together to safeguard global digital infrastructures.

*****

APPLICATION OF IPR IN TODAY'S FASHION INDUSTRY AND ITS FLAWS

Kusuma Rajashekharaiah[35] and Ananya S.B.[36]

ABSTRACT

Style embodies originality, particularly in the realm of fashion, where it represents a distinctive look achieved through cosmetics, accessories, apparel, or other mediums. The fashion industry has grown into one of the most significant industries globally, driven by fierce competition and the desire to stand out. In today's fast-paced world, individuals often use fashion as a tool to express their individuality and differentiate themselves from the crowd. The unique nature of fashion, rooted in human creativity and imagination, demands protection from potential exploitation. Given the rapid evolution of the industry, safeguarding these innovations is essential. The fashion industry is growing daily, with endless possibilities for designers. India, in particular, has emerged as a key global market for fashion merchandise, reflecting its expanding consumer base and creative potential. However, despite the industry's importance, India lacks specific legal provisions that offer comprehensive protection for fashion. Intellectual Property Rights (IPRs) provide some level of security for a designer's original creations, but they often fall short of providing sufficient protection in this dynamic and diverse sector. While IPRs can help shield designs from theft or unauthorized use, the fashion industry faces unique challenges that these laws do not fully address. Designers frequently encounter issues such as copying, counterfeiting, and a lack of enforcement, making it difficult to protect their intellectual property adequately. This article will explore the necessity of stronger protections for India's fashion industry and provide a detailed analysis of the current intellectual protection for original fashion sketches and designs, ensuring that creativity is not compromised in the fast-paced world of fashion.

Keywords: Copyrights; Fashion Industry; Fast Fashion; IP rights

INTRODUCTION

The fashion business is expanding quickly and has seen notable advances in design. Global recognition has been attained by numerous brands and designers, and the industry has a significant financial influence that significantly boosts the growth of the economy of the country. Due to this expansion, there are now a lot of work prospects and a sizable income from the export of fashion items. With people becoming more aware of style globally, fashion now has a significant influence on society. In the era of social media, being stylish has taken precedence. This trend has increased people's desire to buy luxury goods like Christian Louboutin heels or a Prada handbag. Luxury clothes has seen a major increase in appeal thanks to social media.

Many Indian brides dream of owning a Sabyasachi Banarasi saree or donning a Manish Malhotra lehenga for their nuptials. But many people find these expensive things unaffordable, which encourages the creation of knockoffs. Fashion designers are often frustrated by the ease with which knockoffs of their designs can be found everywhere. These knockoffs come in a range of pricing points, from luxury to low-cost.

[35] Student at KLE Society's Law College, Bengaluru, India.
[36] Student at KLE Society's Law College, Bengaluru, India.

The purpose of this research paper is to analyse and study about the enforceability of IPR in Indian Fashion market; also outlining its flaws as well as suggesting recommendations and providing solutions for the problems being faced

THE FAST FASHION INDUSTRY'S PROBLEM WITH DESIGN PLAGIARISM

Plagiarism in design is the act of replicating or mimicking the creative output of another individual. This behaviour is commonly referred to by terms such as "counterfeit," "knockoff," and "piracy". Generating inferior duplicates of clothing that closely mimic high-end designers' or companies' products is known as counterfeiting. This is obviously a violation of intellectual property rights because it copies not just the design but also the brand name.

Adidas sneakers are a common target for counterfeiting. Counterfeit versions are available for as little as ₹1,200 in local marketplaces, despite the fact that an authentic pair may cost up to ₹12,000 there. Since so many sellers are involved, it is difficult to enforce laws against counterfeiting even if it is unlawful. Regulation of this kind appears to be impossible.

People are always on the move in today's fast-paced world, especially in metropolitan regions. Life moves quickly, and this has an impact on the fashion business as well, which has to adapt to new trends. One of the most well-liked business strategies these days is fast fashion, which focuses on mass-producing stylish apparel for profit. Inspired by haute couture, or high fashion, fast fashion manufacturers quickly copy these designs and sell them to the general public at much reduced prices.

Simplified reproductions of designer designs are quickly produced by companies like Zara, H&M, Forever 21, and Mango, frequently before the original designers are aware that their work has been copied. Fashion trends change so quickly that products are often off the shelf by the time designers notice the infringement. Because they operate too quickly for standard regulatory procedures to catch up with, fast fashion firms are challenging to monitor and manage.

RANGE OF THE INDIAN FASHION INDUSTRY

There's an endless scope in the Indian Fashion Industry. From intricate traditional wear for various traditions to casual western wear, The Indian market is diverse enabling brands from all over the globe to pierce through the Fashion market. India's economy is among the fastest-growing in the world, and the country's textile sector has grown significantly over the years. 2012 saw a valuation of ₹720 crores for the Indian fashion sector. According to research, by 2025, the Indian fashion market is expected to develop at a compound annual growth rate (CAGR) of 11–12% and reach $115–125 billion.

Only China has a larger textile industry than India. In addition to bringing in a sizable sum of money, the Indian fashion business employs a sizable number of people in both urban and rural regions. The textile industry's export earnings increased by ₹382 crores in 2018 and 2019. Indian designer clothes made up 1.7% of all fashion exports worldwide in 2020, while traditional handicrafts are exported on a large scale. It is important to remember that the high fashion business offers a substantial number of work prospects, despite the seemingly modest percentage.

Even though it may not be as large as other industries, the high fashion market in India is expanding quickly. The absence of protection for creative designs, however, has drawn criticism. As a result of their work being stolen or replicated, many designers have expressed dissatisfaction that their creative efforts are being undermined. Considering the industry's economic impact and the jobs it creates; it is imperative that the government take action to preserve intellectual property rights and prevent plagiarism in the fashion business. Not only will this help designers, but it will also help the fashion sector in India keep expanding and developing.

INDIAN FASHION DESIGNER'S PROTECTIONS AGAINST INTELLECTUAL PROPERT-Y

Since intellectual property law was first introduced, India has established a number of intellectual property rights. To protect the fashion business, not all of these rights are applicable, though. Since fashion has a strong creative foundation, preserving this industry requires the use of certain intellectual property rights. They are as follows:

Copyrights

In India, the fashion industry is one of the sectors that is protected under the Copyright Act of 1957. Fashion designers have the sole authority to prevent unlawful use of their original designs in this context thanks to copyright protection. The creative, dramatic, musical, and literary works as well as sound recordings and motion pictures are among the media that are protected by copyright under Section 13 of the Act. Although fashion design is not specifically mentioned in the Act, artistic works are covered, which can include fashion articles. The Act defines artistic works as drawings, paintings, sculptures, photos, and architectural designs. Fashion designs are protected by copyright laws since they are regarded as artistic endeavours.

Under the Act, fashion designers have complete ownership rights over their creations and can forbid unauthorized duplication or modification of their designs. As long as a design is original, designers are still entitled to copyright protection for their works, regardless of registration status. Unauthorized duplication, modification, or use of a design in any format—two- or three-dimensional—without the designer's permission is considered copyright infringement. These rights belong to designers and are retained for 60 years following their passing. It is illegal to import, export, trade, or reproduce pirated fashion items without the designer's consent in accordance with copyright laws.

Trademark Protection

India's Trademark Act of 1999 offers crucial protection for fashion labels, allowing them to differentiate their products from others in the market. According to the Act, a trademark can be any mark—be it a name, design, word, symbol, or combination of colours—that distinguishes one brand's products from those of another. In the fashion industry, trademarks serve as the label or logo that identifies a design or brand. This enables consumers to recognize and separate a specific designer's goods from competing offerings. By creating a unique trademark, fashion designers establish a market identity and build brand recognition, allowing their work to stand out in an increasingly competitive industry.

Trademarks are essential for protecting a fashion designer's brand identity and securing their place in the market. They help consumers associate specific qualities or attributes with a particular designer or fashion house, preventing the unauthorized use of brand names or designs. The Trademark Act of 1999 provides designers with a legal mechanism to safeguard their brand, though challenges may still arise in achieving the highest level of protection. Even with the Act's comprehensive definition, intellectual property owners may face hurdles in securing their rights against potential infringement. This means that while trademarks are a powerful tool for protecting a designer's investment, there can still be limitations in fully protecting a brand from unauthorized use or replication.

For major fashion brands, trademarks are integral to their identity and reputation. Well-known logos such as the tiger symbol for Sabyasachi, the horse and chariot for Hermes, or Gucci's double "GG" are instantly recognizable and help maintain each brand's premium status. Trademarks protect this brand equity by preventing others from copying or misusing these iconic symbols. Additionally, trade dress—which covers the size, shape, colour combination, and packaging of a product—also receives protection under trademark law. However, the scope of trade dress protection is largely determined by the courts. A notable case illustrating the complexity of trade dress enforcement is Christian Louboutin v. Abu Baker, in which the court ruled that Louboutin's famous red sole was not protected under trademark law, as a single colour could not constitute a trademark. This ruling highlights the challenges of trademark enforcement, even for globally recognized luxury brands, and underscores the need for vigilance in protecting brand identity.

IPR CHALLENGES AND OPPORTUNITIES IN THE INDIAN FASHION AND APPAREL SECTOR

International luxury fashion brands such as Burberry, H&M, and Richemont made headlines globally when they opted to destroy unsold products valued in the millions. This drastic measure was taken to protect their intellectual property rights and combat the rising tide of counterfeiting. The Indian fashion industry, in contrast, has experienced significant growth and transformation, propelled by the extraordinary creativity and commitment of its designers.

Indian designers are increasingly utilizing local materials, employing traditional coloring techniques, and showcasing distinctive manual design aesthetics, all of which require robust intellectual property protection to ensure their work is not copied or misappropriated. The Indian fashion landscape is diverse, encompassing both established luxury brands and emerging designers who bring fresh perspectives and innovation to the market.

However, the situation varies markedly between these established players and the newer entrants. While many well-known designers and brands have been proactive in registering their creations under IPR laws, the challenges are more pronounced for emerging designers, fashion startups, and traditional textile handicraft sectors. These segments often lack the resources and awareness necessary to navigate the complex intellectual property landscape effectively.

This discussion will specifically explore the intellectual property rights challenges faced by fashion entrepreneurs and traditional textile craft units in India, examining the barriers to IPR registration, the

impact of counterfeiting on their businesses, and potential strategies for fostering a more supportive environment for innovation and creativity within the industry. By addressing these challenges, we can better understand how to protect and promote the unique contributions of India's vibrant fashion ecosystem.International luxury fashion brands such as Burberry, H&M, and Richemont made headlines globally when they opted to destroy unsold products valued in the millions. This drastic measure was taken to protect their intellectual property rights and combat the rising tide of counterfeiting. The Indian fashion industry, in contrast, has experienced significant growth and transformation, propelled by the extraordinary creativity and commitment of its designers.

Indian designers are increasingly utilizing local materials, employing traditional coloring techniques, and showcasing distinctive manual design aesthetics, all of which require robust intellectual property protection to ensure their work is not copied or misappropriated. The Indian fashion landscape is diverse, encompassing both established luxury brands and emerging designers who bring fresh perspectives and innovation to the market.

However, the situation varies markedly between these established players and the newer entrants. While many well-known designers and brands have been proactive in registering their creations under IPR laws, the challenges are more pronounced for emerging designers, fashion startups, and traditional textile handicraft sectors. These segments often lack the resources and awareness necessary to navigate the complex intellectual property landscape effectively.

INDIAN IPR POLICY: THE PATH FORWARD FOR THE FASHION INDUSTRY

India has made steady yet impactful progress in the global fashion landscape over the past three decades, blending the richness of Indian culture with fashion and apparel. Indian fashion remains deeply rooted in its cultural heritage, marked by textiles featuring intricate craftsmanship, delicate designs, and traditional dyeing and printing techniques. These attributes are shaped by the country's distinctive topography and its abundance of skilled artisans, combined with innovative design practices. As a result, Indian fashion has developed a unique identity that distinguishes it on the international stage.

Despite its vibrancy, this industry is highly vulnerable to piracy. While the concept of fashion law is gaining momentum in India, there is still no central law specifically addressing the fashion industry. Nevertheless, the sector's activities, along with its significant environmental and economic implications, have captured the attention of India's legal community.

Current fashion laws in India are inadequate and fail to offer comprehensive protection for stakeholders. In contrast to countries like the USA and France, where fashion law is more advanced, India's regulatory framework is still in its early stages. Consequently, existing laws are expected to evolve, with amendments and new legislation being shaped by input from fashion creators and industry stakeholders. The Fashion Design Council of India (FDCI) plays a key role in advocating for stronger legal protections and is actively working to elevate the reputation of the Indian fashion industry both domestically and internationally, with a focus on sustainability. It collaborates closely with the Ministry of Textiles and the Ministry of Commerce and Industry.

However, enforcing intellectual property rights (IPR) laws to combat fashion piracy is complicated by the rapid expansion of digital media, which poses additional challenges for policymakers in addressing plagiarism. Both established and emerging designers are increasingly dealing with design theft, exacerbated by the visibility social media platforms provide.

Looking ahead, the Indian fashion industry faces numerous challenges, highlighting the need for a robust IPR framework and a standardized code of conduct to address and resolve these issues. Emerging designers and local artisans should be encouraged and guided from the outset to effectively safeguard their intellectual property. By fostering a supportive environment, India can enhance the resilience and sustainability of its fashion sector while protecting the creativity that defines it.

CONCLUSION

The intellectual property rights (IPR) held by a country play a crucial role in shaping its global standing and economic stability. The Indian fashion industry is increasingly capturing the interest of international partners due to its rich and unique textile heritage. However, the current landscape of IPR is facing significant challenges from design piracy and copying, which have been exacerbated by the rise of digital media.

To support the interests of emerging designers, traditional artisans, and established businesses alike, existing fashion laws require essential amendments to enhance their effectiveness. The growing awareness among designers and manufacturers regarding their legal rights demonstrates that IPR laws are beginning to make an impact. Nevertheless, these laws need to be reimagined, ensuring that the process is user-friendly for legitimate creators while being stringent against infringement. By doing so, India can better protect its vibrant fashion sector and foster a more innovative and sustainable environment.

REFERENCES

1. Priyadarshi N, Intellectual property rights: Crucial for fashion industry, International Journal of Law Management & Humanities, 4 (2) (2021) 1545-1549.
2. Chaturvedi S, India: Fashion Industry and Challenges for IP Protection, 2021, https://www.mondaq.com/india/trademark/ 1024232/fashion-industry-and-challenges-for-ip-protection (accessed 8 April 2022).
3. Kumar P, Fashion and Related Intellectual Property Rights, 2019, https://ssrn.com/abstract=3322320 or http://dx.doi.org/ 10.2139/ssrn.3322320 (accessed on 31 March 2022).
4. Chopra A & Biswas R, IPR laws applicable to fashion industry in India, 2018, https://blog.ipleaders.in/ipr-lawsapplicable-to-fashion-industry/ (accessed on 12 April 2022)
5. Karmakar S & Tewari M, Using IPRs to Protect Niches? Evidence from the Indian Textile and Apparel Industry, Indian Council for Research on International Economic Relations, 2014, https://icrier.org/pdf/working_paper_270. pdf (accessed on 10 April 2022).
6. Diwadkar S, India: Role of IPR in The Fashion Industry, 2018, https://www.mondaq.com/india/trademark/704378/role-ofipr-in-the-fashion-industry (accessed on 13 April 2022).

7. Shirwaikar P, Fashion Copying and Design of the Law, Journal of Intellectual Property Rights, 14 (2009) 113-121.
8. Basu R, Fashion, IPR & the emerging designer: IP protection and contractual Safeguards for emerging designers and small fashion firms, 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2635087 (accessed on 11 April 2022).
9. Borkar S, Fashion Law in India, 2018, https://www.khuranaandkhurana.com/2018/12/14/fashion-lawin-india (accessed on 10 April 2022).
10. Agarwal V, IPR registration in fashion industry of India, Journal of Intellectual Property Rights, 24 (2019) 35-40.
11. Bharti S, Legal Protection of Fashion Design in Apparels in India: A Dilemma under the Copyright and Design Law, The Delhi University Journal of the Humanities and the Social Sciences, 3 (2016) 139- 154.
12. Swarup S K & Rastogi S, Fashion Design and Intellectual Property Rights: An Indian Perspective, Journal of Intellectual Property Rights, 26 (2021) 127-135.
13. Sahny P, The Designs Act, 2000: A fashion faux pas, 2012, http://dx.doi.org/10.2139/ssrn.2185519 (accessed on 12 April 2022).
14. Bhatt D, Intellectual Property Law for fashion designers, 2014, https://selvams.com/blog/intellectual-property-law-forfashion-designers/ (accessed on 10 April 2022).
15. Shah A, Registration of shape of goods as Design, 2021, http://www.legalservicesindia.com/article/1348/Registrationof-shape-of-goods-as-Design.html (accessed on 13 April 2022).
16. iGERENT, Intellectual Property in the Fashion Industry, 2021, https://igerent.com/intel lectual-property-fashionindustry (accessed on 11 April 2022).
17. Hilton B, Choi C J & Chen S, The ethics of counterfeiting in the fashion industry: Quality, credence and profit issues, Journal of Business Ethics, 55 (4) (2004) 345-354.
18. Nigam A, India: Significance and challenges of protection to traditional fashion under geographical indications, 2017, https://www.mondaq.com/india/indigenouspeoples/611106/significance-and-challenges-of-protectionto-traditional-fashion-under-geographical-indications (accessed on 13 April 2022).
19. Chavan R, Geographical indications registration system in India, Journal of Legal Studies and Research, 5 (2) (2019) 103-115.
20. Hirwade M & Hirwade A W, Geographical Indications: Indian Scenario, 2006, http://eprints.rclis.org/7878/1/ EF6C0C53.pdf (accessed on 10 April 2022).
21. Press Information Bureau, Ministry of textiles, Government of India, 2019, https://pib.gov.in/Pressreleaseshare. aspx?PRID=1594198 (accessed on 12 April 2022)

*****

SECURE TRANSACTIONS, RELIABLE FUTURE: UNRAVELLING THE COMPLEXITIES OF CYBERCRIME IN INDIA'S E-BANKING SPHERE

Asif Pasha[37] and Milan Donson[38]

ABSTRACT

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

–Newton Lee

The Internet, an intricate global network of interconnected devices, functions as a medium for the exchange of information and connectivity. However, it also harbours a darker side, serving as a platform for 'cybercrime', illicit activities that exploit this technology to gain unauthorized access to data or systems that can target crowds at large, leading to extraordinary losses and hopeless situations. It manifests in various forms and is often transnational and anonymous which complicates the process of identification, tracking, and prosecution of the perpetrators. The e-banking sector is particularly susceptible to cybercrime because transactions often involve third parties, providing cybercriminals with opportunities to interfere unapproved posing a significant challenge not only to technological advancement but also to the protection of individual privacy. In India, traditional banking methods are being rapidly supplanted by e-banking. The transition from conventional crime to cybercrime is both novel and sophisticated since cybercriminals can operate under the veil of anonymity. As economic factors lead to an increase in the amount of money deposited, there is a growing trend towards the use of electronic methods for money storage and transfer. This trend necessitates vigilant monitoring to prevent potential cybercrimes.

Keywords: Cyber Crime, Cyber Terrorism, E-Banking, Technology, Internet.

INTRODUCTION

The world economy has derived into a new scenario of development, courtesy of cutting the Red Tape when our country woke up from its slumber in the most stringent of hours. The Internet revolution has brought the world economy to a new level of advancement. These changes made people advance in every area of life.

Today, the Internet has become an integral part of our daily life. In 2021, there were about 4.66 billion active internet users worldwide, which is about 59.5 percent of the global population. In 2023, India had the second-highest number of internet users in the world, with about 692 million users, which is about half of its population. The Internet accounted for 21 per cent of the GDP growth in mature economies over the past 5 years. Technology has also changed how and where we consume media, how we communicate, and how we tackle global challenges.

RESEARCH QUESTION

- What are the main types and causes of cybercrime in India, and how do they affect the e-banking sector?
- What are the best practices and strategies to enhance the security and privacy of e-banking

[37] Student at Kristu Jayanti College of Law, Bangalore, India.
[38] Student at Kristu Jayanti College of Law, Bangalore, India.

customers and service providers in India?

OBJECTIVE

To analyse the nature, causes, and impacts of cybercrime and cyber terrorism in India, and to evaluate the existing and potential solutions to prevent and combat them in the context of e-banking.

METHODOLOGY

This research utilizes secondary data from diverse sources, including official data, books, articles, journals, reports, magazines, newspapers, and websites, to analyse the evolution of banking and e-banking. Qualitative methods such as content analysis, thematic analysis, and comparative analysis are employed to examine the data. The paper also analyses regulations and their outcomes in combating cybercrime and cyberterrorism in the context of e-banking. The findings are interpreted to identify trends, challenges, and opportunities, and provide recommendations for enhancing security measures and regulatory frameworks in the e-banking sector.

E-BANKING

One of the most important aspects of our life that has been transformed by the Internet is money which allows us to manage our money anytime, anywhere, without any hassle and uses the Internet as a platform to deliver various services to customers. It has many benefits for both banks and customers, such as lower operational costs, higher convenience, faster transactions, and easier access to information.

The advent of digital payments and online banking, which are subsets of E-banking, has transformed the banking sector in India. The demonetization period in 2016 gave a boost to the adoption of digital payments, which were initially promoted by international banks. E-banking involves various types of digital payment methods, such as banking cards, mobile wallets, UPI, and AEPS, which have different features and benefits for users. It offers various benefits such as fund transfers, bill payments, deposits, account statements, and product orders.

People prioritize their comfort over the potential consequences they might face in the future. During the COVID-19 pandemic, internet banking became an integral part of daily life in India. It has become an advantage for many working in the online banking sector, as e-banking provides a safe way to conduct transactions such as paying bills and fund transfers. This trend is not likely to decrease anytime soon. Internet banking has revolutionized the way we manage our finances. As a result, it offers convenience, simplicity and efficiency in our daily lives. For example, we can access our accounts, transfer money, pay bills and check statements online anytime and anywhere. Therefore, banks use electronic media to provide a wide range of services that save time and resources.

Internet transactions have become a major mode of trading and individual transactions in the country, offering the cheapest way of providing banking services. However, e-banking services also entail risks along with benefits. For instance, they may expose customers to cyberattacks, frauds, or technical glitches. Despite these challenges, e-banking enhances the speed and convenience of transactions and

makes life simpler and happier. As more people join the net, the risks and opportunities of e-banking will also grow. Therefore, this problem needs to be addressed to ensure the future of net banking.

With a variety of options ranging from e-banking to mobile wallets, Asia is transforming the way people pay and get paid and is a pioneer in the field of digital payment solutions, having embraced them for almost a decade now. While Visa leads the E-Banking market, it faces tough competition from mobile payment options which is only poised to grow in the years to come.

While China, Korea, Japan and the SEA region were after this trend, with the introduction of a Uniform Payment Interface (UPI), India's dream of a cashless digital economy gained traction. UPI was adopted fairly quickly by the masses as a healthy consequence of events like overnight Demonetization which was further propelled by the Coronavirus Pandemic, which encouraged people to incorporate digital technology into their daily lives. As a result, digital payment has become a key mode of E-Banking for many Indians, although cash is still the king, it could soon be dethroned.

However, E-banking also comes with many challenges in the modern world. Despite the rules and security measures in place, it is not immune to cyber threats and risks, such as cybercrimes, security breaches, technical glitches, and customer dissatisfaction. Therefore, e-banking requires careful management and regulation to ensure its safety and reliability. Although E-banking is a convenient and cost-efficient way of accessing banking services through the Internet, it also has some drawbacks that may discourage some customers from using it.

CYBERCRIME

Internet transactions have become a popular way of conducting financial transactions, providing a cost-effective alternative to traditional banking services. However, the convenience of e-banking comes with certain risks, such as cyberattacks, frauds, and technical glitches. Despite these challenges, e-banking has made transactions faster and more convenient, simplifying people's lives. As more people adopt e-banking, the risks and benefits will continue to evolve, requiring ongoing attention to ensure the future of this mode of banking.

These cybercrimes are carried out by hackers who breach computer networks or systems to manipulate, steal, or destroy data, disrupt services, or take over the system. They may target individuals, businesses, or government entities for various motives, such as financial gain, political agenda, personal vendetta, or thrill-seeking. These cybercrimes violate the rights and dignity and expose to physical and mental harm. Specialized law enforcement units are working to prevent and prosecute these horrific crimes.

Security is the main concern and challenge of net banking. However, if proper safety measures are adopted, this issue can be resolved. For example, some banks have come up with innovative solutions to enhance the security level at every stage of the transaction, such as virtual keyboards and new grid-based debit cards.

To address the risk factors and challenges of online banking, RBI has issued guidelines to all banking institutions, advising them to take necessary steps to control this section of online banking. Moreover, the central government/RBI has made various provisions to solve the problem in banking sectors, such

as recruiting young and capable recruits who have specialized knowledge in the field of technology. The growth of Internet banking has also prompted many to rethink their information technology strategies in the competitive market.

The Reserve Bank of India (RBI) has issued several guidelines to ensure the security of financial transactions.

- Firstly never share account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card / credit card details with anyone, even bank officials.
- Secondly, be cautious of any phone call or email threatening the blocking of account due to non-updation of KYC. Always access the official website of the bank or contact the branch for any updates.
- Avoid downloading unknown apps as they may secretly access confidential data.
- Remember that transactions involving receipt of money do not require scanning barcodes or entering MPIN.
- Always access the official website of the respective bank for contact details and to be wary of fraudulent contact numbers on internet search engines.
- Check URLs and domain names received in emails or SMSs for spelling errors and use only verified, secured, and trusted websites for online banking.
- If you receive an OTP for a transaction not initiated by you or a debit SMS for a transaction not done, inform your bank immediately.
- Do not share the password of your email linked to your bank account and avoid having common passwords for e-commerce or social media sites and your bank account.
- Do not set your email password as the word “password” or something very simple while registering on any website or application with email as user-id.
- Be wary of misleading advice intimating deposit of money on your behalf with RBI for foreign remittances, receipt of commission, or wins of lottery.
- Regularly check the email and phone messages for alerts from your financial service provider and report any unauthorized transaction observed to bank immediately.
- Lastly, secure your cards and set daily limit for transactions. You may also set limits and activate or deactivate for domestic or international use.

Fiscal fraud is a form of cybercrime that involves illegally obtaining confidential financial information. Some examples are:

- Credit card fraud: Using someone else's credit card details to make unauthorized purchases or withdrawals.
- Identity theft: Stealing someone's personal information, such as name, date of birth, or social security number, to open accounts, apply for loans, or commit other crimes in their name.

- Phishing schemes: Sending fraudulent emails or messages that appear to be from legitimate sources, such as banks, companies, or government agencies, to trick recipients into revealing their passwords, account numbers, or other sensitive data.
- Online banking fraud: Accessing someone's online banking account without their permission and transferring funds, paying bills, or changing settings.

These cybercrimes can have negative impacts on the e-banking sector, such as:

- Loss of customer trust and confidence in the security and reliability of e-banking services.
- Financial losses due to unauthorized transactions, refunds, or compensations.
- Legal liabilities and reputational damage due to data breaches or compliance violations.
- Operational disruptions or downtime due to cyberattacks or system failures.
- Increased costs for cybersecurity measures, insurance, or recovery efforts.

India is one of the top countries with the usage of the Internet. People in the country are compelled to use Internet services due to certain situations. E-banking in India has a bright future. There are many opportunities in e-banking. So, there will be a situation of misusing it. So, people who are using internet services like banking, e-commerce etc. should be aware of the privacy and security provided by the network. The negative side of net banking has become a challenge for the future. There should be proper rules and awareness of e-banking. If anything happens that is not accepted by the services, try to inform the consent authorities as soon as possible.

SUGGESTIONS

The existing rules are not sufficient to protect crores of people in the country from fraudulent activities in online banking. Internet Banking in India needs effective support to build the infrastructure for secure banking. The technical issues are still a threat to the security of Internet Banking. Tampering the websites and making fake websites all these issues will make the environment insecure. The hosting sector should itself need to focus on demonstrating and giving methods for the effective and secure use of online banking.

The study revealed that there is no way to completely eradicate cybercrime in the financial industry. Yet by assuring some fundamental security incentives from the bank to promote criminal activity in the approaching automated environment, it can limit its spillovers.

- **Better Authentication Techniques**: Banking institutions should investigate and use sophisticated authentication techniques that go beyond conventional passwords and 2FA. This could use behavioural analytics that examine user behaviours to find abnormalities or biometric authentication methods (like fingerprint or face recognition).
- **Continued Improvement of Encryption Protocols**: To safeguard sensitive data while it is being sent, online banking systems employ encryption techniques that are constantly improved. To keep ahead of new threats, use encryption algorithms that are industry standard and guarantee that they are updated often. Constant Monitoring and Fraud Detection Invest in

reliable monitoring solutions that can spot shady activity in real time. Use machine learning and artificial intelligence techniques to spot trends of fraud and proactively halt unlawful transactions.

- **Multi-Layer Security**: Put into practice a multi-layered security strategy that consists of firewalls, intrusion detection systems, and anti-malware programs. Perform routine security audits and penetration tests to find weaknesses in the net banking infrastructure. Address any flaws immediately, and ensure security fixes and upgrades are deployed often.
- **Customer Awareness**: Financial institutions should give client education and awareness campaigns top priority. Inform clients often about security best practices, typical risks, and how to keep secure when using online banking services. Users may benefit from this by learning more and taking greater initiative to safeguard their accounts.
- **Collaboration Efforts**: Encourage cooperation between banks, industry regulators, and cybersecurity specialists to exchange knowledge about new risks and effective practices. Rapider response times and more potent mitigation measures may result from this coordinated approach.
- **Regulatory Framework**: For online banking, governments and regulatory agencies should create and enforce strict security standards and laws. To secure consumer data, financial institutions must maintain a high degree of security and use standardised procedures.
- **Incident Response and Customer Support**: To handle security problems quickly, create a detailed incident response strategy and a dedicated customer support system. Be sure to promptly resolve any security-related concerns and provide clients with clear advice on how to report any suspicious activity.
- **Ongoing Security Training**: Inform bank staff members and employees regularly about the newest security risks, social engineering strategies, and best practices for protecting client data. Banks may lessen the risk of internal security breaches by retaining an informed and security-conscious workforce.

Internet banking is the cheapest way of providing banking. Internet banking is increasing, and it has become a “need to have” than a “nice to have” service. But there is still some traditional system in banking like cheque, cash withdrawals, etc. The digital world promotes digital services. The rules and laws will not provide complete protection. The awareness of society and individuals about the pros and cons of Internet banking is the basic importance.

CONCLUSION

The internet is a web of wonder that can bring us many benefits and opportunities. But it is also a web of woe that can expose us to many harms and hazards. We need to be careful and responsible when we use the internet and not let cybercriminals ruin our online experience. The main challenge is security and privacy. Even though there are security measures issued by the bank authorities, they are not helpful in the future. The main step that everyone can take is that be aware of what they are doing on the internet

and aware of the application used. The internet is what we make of it. Let's make it a safe and positive place for everyone.

Cyberterrorism is the use of digital technology to conduct terrorist activities, such as attacking critical infrastructure, spreading false information, or conducting espionage. Cyberterrorists may aim to cause fear, chaos, damage, or death among the public or specific groups. Cyberterrorism poses a serious threat to the security and stability of society.

Another form of cybercrime is cyberbullying, which is the use of internet platforms to harass, intimidate, or blackmail someone. Cyberbullies may use social media, instant messaging, or email to spread rumours, share embarrassing images or videos, or engage in online harassment. Cyberbullying can have serious psychological and emotional consequences for the victims, such as depression, anxiety, low self-esteem, or suicidal thoughts.

*****

THE ROLE OF GENERATIVE AI IN AUTOMATING THE RESEARCH PROCESSES

Sangbit Roy[39] and Subhayan Basak[40]

ABSTRACT

The introduction of Generative Artificial Intelligence (AI) technologies, especially advanced language models called "LLMs," has initiated a colossal shift in academic and industrial research methodologies. This paper explores the transformative impact of generative AI on automating various facets of the research process, including literature reviews, data analysis, hypothesis generation, and preliminary drafting. Researchers can significantly speed up time-consuming tasks by leveraging machine learning algorithms capable of understanding and producing human-like text, allowing greater focus on critical analysis and innovation. Additionally, generative AI facilitates the synthesis of vast amounts of information from diverse sources, enhancing the comprehensiveness of research outputs. The integration of generative AI not only enhances efficiency but also introduces novel perspectives by uncovering patterns and insights that may evade detection from human researchers. However, this technological advancement brings forth challenges and ethical considerations, such as the accuracy and reliability of AI-generated content, potential biases in algorithmic outputs, intellectual property concerns, and the possible erosion of essential research skills. Furthermore, the reliance on AI tools may impact the traditional dynamics of collaborative research environments. This paper critically examines these issues and proposes a balanced framework for integrating generative AI into the research workflow. Emphasis is placed on the necessity of human oversight and the development of ethical guidelines to ensure that AI is a tool to augment rather than replace human intellect. The study aims to comprehensively understand how generative AI can be harnessed to enhance the research process while mitigating associated risks, ultimately fostering a symbiotic relationship between human researchers and artificial intelligence.

INTRODUCTION

Moving from theory to practice, AI has transformed from a buzzword into an important technology applied across industries, from healthcare and finance to transportation and law. In the legal context, AI serves to enhance efficiency by automating mundane tasks in document review, predictive analytics, and contract analysis, thereby freeing up professionals to deal with issues needing greater complexity.

AI's integration in law streamlines operations, reduces costs, and improves accuracy by processing large volumes of legal data and predicting case outcomes. However, it raises concerns around job displacement, biases in algorithms, and the transparency of AI-driven decisions, demanding careful regulation and ethical oversight.

This research has tended to focus on exactly how AI is going to impact research into matters of law, judiciary processes, and the enforcement of laws—both in challenges and benefits. This work has covered issues dealing with bias, privacy, and ethics, and proposed strategies for the ethical use and integration of AI in practice.

[39] Student at The West Bengal National University of Juridical Sciences (WBNUJS), India.
[40] Student at The West Bengal National University of Juridical Sciences (WBNUJS), India.

It specifically touches on main study areas: cybercrime, intellectual property, law enforcement, and judicial uses of AI. Materials are combined in literature review, case studies, and statutory analysis, taking into consideration jurisdictional differences. The research aspires to present an overall analysis while pointing out limitations brought in by the fast movement development of AI, which may render findings sensitive to time.

AI-POWERED ROBOTICS AND CYBER CRIMES

What are AI powered robots?

AI powered robotics refer to the integrated with artificial intelligence technologies, that enable them to perform tasks autonomously by perceiving their environment, making decisions and learning of experiences. The key features of any AI based robotics include machine, sensory perception and autonomous navigation, which allow the AI powered robots to interact adaptively, with their dynamically shifting surroundings.

More recently, developments in the fields of autonomous vehicles, drones and industrial robots have seen a significant boom. For example, entire conflicts like the Russo-Ukraine war have been majorly played with self-reliant, AI-powered attack drones, while on the other hand, self-driving cars increasingly use AI for real time decision making on the move instead of relying on rigid and preordained computer codes set in the factories. These are widely regarded as the fruits of the development of advanced machine learning, that learn the tasks through demonstration and trial and error training, instead of relying on hardwired programming coded into it.

Emerging Role of AI in Cyber Crimes:

In a wider perspective, the open access to AI resources and development can enable cybercriminals to execute sophisticated attacks with great efficiency. Although not new, “Deepfakes” are a basic AI powered synthetic media generating technology is now enhanced by the rapid development of AI ecosystem. This technology has been used to create realistic videos with accurate voices to replicate real people, particularly for frauds and scams. There are even AI driven tools that hack a system to scan for vulnerabilities, adapt to the existing security measures and launch fully automated hacking attacks.

The scale and complexity of the capabilities of AI driven cyber threats are increased even more by its capability for automation. An AI model specifically trained for such purposes can process vast amount of data, identify potential targets and bypass security systems, without any need of human intervention in between.

Legal Challenges in Addressing AI related Cyber Crimes:

Determining the responsibility for AI propagated cyber crimes poses a significant challenge. Significant questions of law regarding the liability arises in such cases, where it needs to be determined who is responsible, the developers of the AI, the users of the AI who deployed it, or a new frontier entirely – should the AI itself be held liable. A reasoning for such being that AI is an intelligent program capable of autonomous decision making.

These types of cyber crimes also transcend geographical and political borders, and AI's global reach exacerbates jurisdictional complexities. Prosecuting perpetrators of AI driven cyber crimes become difficult when it involves multiple different countries with different laws, regulations and jurisprudence regarding such crimes. Therefore, courts have struggled with the new wave of cyber crimes attacks, dealing with a lack of legal precedents regarding such cases, especially in a system of precedents like the Indian judiciary. Judicial Systems however, have begun to recognize the need for a change, the need for updated laws, but comprehensive changes remain in development.

ROLE OF GENERATIVE AI IN AUTOMATIC RESEARCH PROCESSES

A brief introduction of generative AI:

Generative AI has brought in a new resurgence in the development of AI platforms, which brings forth an entirely different method of utilising AI programs. Generative AI are AI models that creates and compiles data in form of text, images and more, based on patterns learned from an existing dataset. ChatGPT, Midjourney and DallE are some of the most advanced examples of such technology. These models can generate text and images, interpret and solve problems, and synthesize information from vast sources of data. These extensively dataset-trained models through sets of fine tuning and learning become capable of producing coherent and relevant response to a wide array of user generated prompts.

Transforming the field of Legal Research:

The use of emerging technologies like Generative AI in legal research field has significantly transformed how legal professionals might approach the stage of information gathering. Normally, and colloquially, legal research has required the patience of combing through numerous documents, cases, statues and bare acts. In the age of computer, the same work has merely shifted to browsing internet sources. However with a generative AI trained on vast amount of legal research, precedents and research methodology, such work can be offloaded to the AI program. This reduces the time spent sifting through potential research material by directly targeting the relevant material, making the entire process much more time efficient.

Ai can also enable direct access to legal resources that would earlier be time consuming or difficult to find by the virtue of being obscure. By automating these processes, AI tools ensre that the Legal professionals can focus on the higher level strategic tasks.

Ethical Concerns and Other Challenges of AI Powered Research:

Despite the efficiency, the use of generative AI in Legal research brings forth well founded concerns. One such problem causing such concern is the susceptibility of the AI to "hallucinate", where it often confidently makes up fake, incorrect information believing it to be correct, to complete the tasks, often to mend the shortcomings due to any technical inability. This alone, raises crucial questions over the accuracy and reliability of such models.

For such reasons, Human oversight remains a crucial step to ensure the accuracy of such works:

Other concerns regarding the AI bias also remains significant. At the end of the day, the AI itself would only act as partial as it is trained to be. If the training dataset of the model is biased, it can lead to a

distinct bias in the program's results. In the field of legal research, such bias and unfairness can undermine the base of the research, especially when applied in socially sensitive areas like civil rights or criminal laws.

Further concerns about violation of Intellectual Property rights also arise, where AI generated content has raised issues of ownership and the potential to infringe the copyrights laws, more so when they're used to draft legal documents.

Impact of AI on Legal Professionals:

The advent of AI models like GPT-4 of ChatGPT is pushing the legal professionals today to adapt their skill sets to best utilise the rising new technology. A focus on Analytical and Critical Thinking is required more than the capability to perform repetitive research tasks. Mastery over such new tools can skyrocket a legal professional's ability to apply the knowledge to their work.

However, Human oversight and supervision to the programs remain indispensible; in order to ensure compliance with the ethical standards, as such has yet to be automated.

ENFORCEABILITY OF IPR PROTECTION LAWS IN THE DIGITAL ERA

Intellectual Property Rights in the Digital Era:

The wide shift to digital media has profoundly impacted the creation and distribution of intellectual property, which has been aided by the internet. Creators can now easily distribute their works globally. But this has opened doors to unauthorized uses of such IP. The ease of access to digital content on the internet has allowed users to copy and share the content without proper authorisation, which has exacerbated the problem.

AI and Intellectual Property Rights:

AI's increasing role in creation of unique content invites questions about its origin and ownership. Under the contemporary IPR laws, only humans are recognised as authors, owners and inventors. This has stoked debates over whether AI generated content, specifically in the field of arts and multimedia, would be eligible to invite the review and expansion of the current laws.

On the other hand AI security solutions can also offer solutions to IP infringements. AI powered tools can monitor the vast amounts of online content which come under the ambit of IP protection, and identify the violations like unauthorised copying and production of counterfeits. Such solutions can prove to be critical to address the rapid spread of the problem in the vastness of the internet platforms.

Challenges in Enforcement:

One of the most significant challenges in enforcing IPR laws in the digital era is the global reach of the content via the internet. Furthermore, the anonymity of the online perpetrators and the entire "whack-a-mole" phenomenon that follows, where the same illegal content keeps reappearing under new links and sites makes it difficult to track and hold the infringers accountable.

Moreover, evasion strategies like VPNs, end-to-end encryption and dark web platforms allow the infringers to evade detection relatively easily, and give them a free reign to distributed illegal and counterfeit products obtained through IPR violations.

Policies and Legal Responses:

Given the challenges that exist, the urgent need to modernise the IPR laws to address the issues related to AI and digital infringement of IPR arise. Legislative updates are required to clarify ownership of AI generated works and ensure that digital content creators have the tools necessary to protect their IP in the digital realm. For such International cooperation is extremely essential for effective enforcement. Treaties like the World Trade Organisation's TRIPS agreement aims to establish minimum standards for IPR laws, facilitating cross-border enforcement. Collaborative efforts between the governments are also crucial in combating such problems, ensuring that IP Rights are protected globally.

SOCIO-LEGAL IMPLICATIONS OF AI INTEGRATION IN COURTS OF JUSTICE

Application of AI in Judicial Processes:

The solutions offered by AI have the potential to improve the efficiency and decision making of the courts. Predictive Analytics is one such application, where the AI is allowed vast datasets such as precedents, cases histories and their outcomes, and extensively trained on it to predict the outcome of cases. Through this, AI can provide insights into judicial decisions by comparing the present case to past rulings, which will aid the judges to make informed decisions. Such technology has already been employed in Australian Family courts to settle divorce cases and asset distributions in such.

Additionally, AI enhances the administrative efficiency by automating tasks like management of courts schedules and cases. AI can help streamline the processes and help courts manage and prioritize cases based on its urgency and complexity. This allows the most efficient utilisation of time and allocates human resources proportionally to cases.

Ethical and Legal Concerns:

Despite the benefits of such a system, one cannot overlook the significant ethical concerns presented by it. One major issue can be the algorithmic bias of AI, where the AI systems perpetuate the existing social biases fed by the training data instead of alleviating them. For example, in the US the historic racial profiling of the police can feed the predictive AI algorithms with racial bias. Similarly, if implemented in India, it may feed on the caste and religion biases of the society.

The "Black-Box" problem may also present itself in such situations.AI decision-making programs can often be opaque in their processes. This can make it difficult for judges, lawyers and professionals to understand how such decisions were made. In US cases of State vs. Loomis (881 N.W.2d 749 (Wis. 2016)), the defendants challenged the AI-based sentencing, as the working behind the program couldn't be fully grasped by those who used it.

There still remains a critical distinction between human judgement and AI however; as such decisions often lack the human touch. Nuances like empathy, morals and a deeper understanding of the unique context in a present case cannot be understood by AI algorithms, yet. AI strictly works on the analyzed

training data and predicts the outcome based on its calculations. It falls flat when a nuanced human take is required to address in a case to dispense proper justice. Hence, human oversight again proves a necessity in such cases.

Public confidence in AI augmented justice:

The trust of the larger population is essential for building the legitimacy of AI's place in the judiciary. AI's perception in courts have brought a mixed result, with some seeing it as a tool to boost efficiency while others fearing the erosion of human elements of justice. Therefore, the foremost requirement of building public trust is to ensure transparency and ensuring that AI compliments, rather than fully replace, any human roles in the judiciary. Trust-building measures are hence crucial, such as regular audits of such systems, ensuring algorithmic transparency and also allowing the opportunity to challenge such decisions, in order to foster trust in AI augmented justice.

THE ROLE OF POLICE IN INVESTIGATING DIGITAL CRIMES

Evolving Nature of Digital Crimes:

The digital era has transformed traditional crime heavily. Giving rise to new threats like ransomwares – where attackers hold, often crucial, data hostage in exchange for a ransom, spywares and cyber espionages – where state sanctioned or non-state actors spy through personal devices and steal sensitive data and information for geopolitical or financial gains. Cybercriminals exploit sophisticated AI tools to automate such attacks, such as phishing schemes and malware distribution, making such crimes harder to detect and investigate into.

AI tools to help Law Enforcement:

To combat such growing threats, the law enforcement agencies, especially in India are adopting AI-powered surveillance technologies. AI based facial recognition systems and data analysis tools are employed to identify and track criminal activities. The inclusion of AI allows these systems to analyze a vast amount of data and look for issues through surveillance systems in real-time, allowing police to detect and prevent crime through recognising patterns that would be normally overlooked by humans manually using these systems. Such predictive policing models can help identify criminal hotspot and find suspects and potential offenders before the crime even occurs, which gives the police force more breathing room and allocate their resources properly.

Ethical and Legal Implications of AI powered policing:

The use of AI rightfully raises serious concerns about privacy. Excessive surveillance using such powerful systems may fail to balance the scales between individual privacy and fundamental rights, rightfully transforming into a "surveillance state". India's new criminal laws – the Bharatiya Nyay Sanhita (BNS) and Bharatiya Nagarik Surakhsha Sanhita (BNSS) emphasize the collection of digital evidence, while also raising concerns over the usage of the data and its protection from misuse.

Such systems can also fall into similar bias problems as the previously discussed AI models which help the judiciary. Instead of mitigating discrimination, the policing AI models may replicate and reinforce

it, due to the faulty training data, targeting specific socioeconomic or ethnic/racial groups disproportionately.

Training and Capacity Enhancements:

The effectiveness of digital crimes also depends on the training and skills imparted to the police force. The increasing need of the hour is the development of Digital Forensics and AI technology skills by the police to handle the complexities presented by cybercrime cases.

At the same time, resource allocation remains a challenge, as the implementation of AI-based tools and digital forensic capabilities require significant investments of such resources into technological infrastructure and development. With the ongoing reform of India's criminal laws, the government is expected to increase investments in these areas, ensuring that the police are ready with sufficient resources in this digital age.

CONCLUSION

This research paper having thoroughly examined the multifaceted role of AI in the legal has demonstrated the development of AI, from its early stages to current widespread applications, which have given rise to its entry into the legal arena. AI has demonstrated the ability to transform the field of Legal Research and Court cases, by inducing efficiency in document review and also play a part in predictive analysis of a case. New AI inventions like Generative AI tools can streamline the tasks in the review of legal texts and precedents by automatically vetting the sources to find the most relevant ones, providing accurate results and improving the efficacy of time allocation.

However, AI's integration into legal practices also brings about its fair share of challenges. AI's inherent bias based on its training data and questions about upholding the fairness in trials raise significant concerns. As such, instead of perfecting the established mechanisms, it may perpetuate the prejudices. At the end, AI just as accurate and fair as its training data. Ethical questions have also been about the potential of AI being misused for cybercrime, violating IP rights. The need for continuous need for human oversight on the usage of AI highlights what's the dual-edged sword, which is AI.

However, looking ahead we can expect AI's role in the legal field to grow, not only in the areas of Intellectual Property and Cybercrime laws, but also through its application in the judiciary in a more direct format. The growing reliance over AI necessitates the preparedness from professionals in this field – Lawyers, Judges, Police Officers etc, to ensure that problems in transitioning doesn't raise issues of adaptability.

*****

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN INTERNATIONAL AVIATION: A CRITICAL STUDY

Sidhant Gupta[41] and Sunavo Ray Chowdhury[42]

ABSTRACT

Artificial Intelligence (AI) will provide the aviation sector with $8 billion in operational efficiencies by 2022. The implementation of AI in Aviation could minimize human-error and other risks. This paper investigates the legal viability of the implementation of Artificial Intelligence in Commercial Aviation, it further includes the examination of the central structural treatise on the topic, the study of regional Bilateral Aviation Agreements, and Multilateral Agreements (Mas). To identify the lapses of the current laws and identify policy-spaces. The paper contains a review of the existing literature, analysis of key trends and developments of international law, and a corelation with the International Law harmonization efforts. Part I of the paper lays down the definition of AI and its scope in aviation. Part II of the paper investigates the International Legal Framework for Aviation, existing legal regimes and 'Structural-Regimes' of International Aviation Law, Bilateral Investment Treaties and MAs. Part III investigates the existing liability mechanisms and its viability for suitable implementation of AI into Aviation. Part IV presents Data-Protection and Privacy related concerns arising out of AI implementation. Part V supplements the paper with the most relevant case studies. Part VI presents the future trends and challenges into the implementation of AI in aviation. Part VII of the paper presents the conclusions and the policy recommendations. The study concludes, based on the analysis of the relevant aviation law, that the way forward is to implement AI related nomenclature and Data-Privacy related specific concerns as 'minimum standards' in the model BITs and MAs, as a part of the harmonization efforts so that the liability regimes and multiple other forms of dilemmas could be effectively resolved. There should be a centralized legal framework consisting of the major aviation stakeholders a regulatory authority. Every automation effort should have a human supervisor to minimize overall risks and dilute the AI liability dilemma.

Keywords: Aviation Law, Artificial Intelligence, International Investment Law, Bilateral Investment Treaties, ICAO, Data Privacy.

INTRODUCTION TO AI IN AVIATION

Artificial Intelligence (AI) is gaining significance by the day, generative AIs and Large Language Models are being used in various fields save for an extensive implementation in the Aviation Industry. AI technologies may provide the sector with an estimated $8 billion in operational efficiencies by 2022. In present-day if, all the pilots of an aircraft have been incapacitated it would mean that all the lives on board will be lost but, with usage of a properly trained AI, the day could be saved. The AI technologies can enhance Aviation in multiple ways for instance, support efficient air traffic flow management, aircraft servicing, or passenger service. AI can supplement the tasks of the human counter-parts from pilots to even ground staff.

An introduction of AI to aviation raises a number of legal questions, there are a number of gaps in the judicature which need to be addressed. The primary focus of this paper is to analyse how the established legal regime of aviation supports the idea of implementation of AI or stands against it. The paper is

[41] Assistant Professor of Law at Vellore Institute of Technology, A.P., India.
[42] Student at Vellore Institute of Technology, A.P., India.

formulated as a purely doctrinal research paper, as a critical study of the established norms through a comprehensive analysis of existing international and European guidelines, regulations, and directives, as well as reports, guidelines, and statements published by relevant independent bodies.

Definition and Scope of Artificial Intelligence in Aviation

Artificial Intelligence (AI) in aviation has no strict proven definition yet, though some research works define it rather broadly as a system with learning capabilities, irrespective of special linkages to the aviation domain in which it is applied. On the other hand, it is also argued that AI covers a variety of diverse concepts, including self-regulating systems, machine-learning, cybersecurity interventions, and softwares that are able to adaptively engage in their surrounding environment. As per the existing scholarships studies on the application of AI in aviation are confined to implementing AI as an overarching term for the different AI concepts and technological tools such as, automated systems, robotics, high-level data systems, and advanced analytics. It further includes predictive-maintenance, air-traffic management, security, filtering, baggage handling, sensor data analysis, flight optimization or intelligent-engines, dispatch reliability, consumer services or robotics, operations of drones and unmanned systems for landing. On this premise the linkages of AI and Civil Aviation have the promise of becoming a very effective and optimized system, in terms of both cost and time but at the same time it there is no space for mistakes as even the smallest mistake in this sector could mean the loss of many lives.

INTERNATIONAL LEGAL FRAMEWORK FOR AVIATION

The international legal framework for air transportation consists of more than 12 conventions and 19 annexes developed by enacting global standards. Thus, there is a very substantial legal basis upon which the analysis of implementation of AI in aviation has to be conducted upon. The primary documents that regulate the legal premise of Civil Aviation are Chicago Convention on International Civil Aviation (1944), ICAO Annexes, ICAO Regulations, and all the other framework that has been laid down by ICAO, other than that, specific routes are regulated by BITs and Multi-lateral Agreements (MLAs) like erstwhile NAFTA and USMCA and etc. Also, the International Federation of Air Line Pilots Associations (IFALPA) Standards and International Air Transport Association (IATA) Regulations are additionally important. This section of the paper gives a brief summary of the various international documents that might bear upon the incorporation of AI into aviation. The 1944 Convention on International Civil Aviation established the organization and authorized it "to adopt all practical measures that may be necessary or expedient ... for the safety of air navigation and the regularity of air transport". The formation of the International Aviation law is such that the enforcement of jurisdiction depends on a number of things, including location, state of the aircraft-owner, state of registration, state of the operator or state of the leasing, state of the occurrence or the action committed has a 'connection factor' with the state concerned. Although the requirement of the existence or creation of a connection is key to the rule, the notion is not defined in the treaties and the intentional usage of extraterritoriality of flight status in the committing of the crime is also not covered by the texts. In these scenarios it is the regional aviation agreements that appropriate the primacy, e.g., the European and U.S. regional

agencies, for example, both give weight to foreign approaches when considering high-level, system, and higher risk regulations.

The primary reason behind the above discussion was to elucidate that the implementation of AI in global civil aviation does not conform to one document or one piece of legislation, there needs to be taken a sectoral or regionally conformist approach based on the regional Multilateral Agreements (MLAs) or specifically useful Bilateral Agreements. In the event of conflict of approaches, it is so far beyond a doubt that AI systems are not, categorically, approved but at the same time they are not disapproved, which puts them in a grey area. As aviation industry is subject sectoral regulations, it is compliance to those regulations that would permit the use of AI systems.

International Civil Aviation Organization (ICAO)

Sustainability of global air transport is an important goal. It is the task of the International Civil Aviation Organization "to promote safety, the safety of flight operations, efficiency, regularity, and the planning of air transport." The ICAO's legal mechanism makes it possible to create an enabling environment for the use of AI technologies in aviation however, with the consent of the state parties involved. The state parties need to develop technical co-operation by providing assistance, sharing relevant practices and by creating a recommendations system for the effective implementation and creation of guidelines.

For these purposes the inter-state co-ordination and harmonization of the relevant legal framework are needed. Consequently, in order to discuss the integration of AI in the policies of modern civil aviation. As such it should be emphasized that harmonization might very well be the key to successful implementation of AI into aviation. These parameters result from the ICAO's co-ordination, research, and development efforts. Due to the ICAO's framework with respect to the obligations of the Member States for the implementation of SARPs, it is necessary to consider an appropriate ICAO mechanism to address this field, in particular, given the legal aspects of this integration in the aviation field. There will arise a number of disputes or disagreements amongst the state parties and for the effective resolution of the same within the ICAO mechanism itself there needs to be a Dispute Resolution mechanism, for disputes regarding AI, and inclusion of such Dispute Resolution mechanism must be within all the BITs and MAs, preferably construed as 'minimum standards'.

Regulation and Oversight of Artificial Intelligence in Aviation

In the aviation sector, robust regulation and oversight mechanisms are in place to ensure safe and secure operations. Regulatory authorities and organizations are tasked with setting and monitoring compliance with international or regional standards and best practices in relation to, in particular, the airworthiness of aircraft, their systems, equipment, and parts, as well as the fitness of the crew and air traffic controller. This area of the law is highly complex and has developed extensively in specific national legal systems, but it also now includes many international treaties and agreements that regulate the various international aspects of civil aviation. In the recent past, new and adapted rules have been developed and implemented to regulate, in particular, the use of drones and electronic identification of aircrafts. AI is based on machine learning and can self-improve by using and analysing data. Due to this there is a serious co-relation between AI implementation and Data Privacy related concerns in the Aviation due

to which there is a potential of rise of serious ethical concerns relating to the usage of AI in aviation. A number of such issues have also surfaced. No doubt the legal and regulatory questions are often complex and difficult. They often deal with uncertain predictions and balance conflicting and many times undefined rights and interests. They often challenge economic and safety concerns and require that the difficulties of the legal regime interact with deep scientific hypotheses. As such, advancement in the law and the way scientists and engineers react to it will help shape the direction and speed of AI in aviation.

Regulatory Authorities

Several players are involved in the regulation of AI technologies in the aviation sector. At an international level, two key authorities play a specifically relevant role. One is a specialized agency of the United Nations, whose role is to set the standards and regulations necessary for aviation safety, security, efficiency, and regularity, as well as for the environmental protection of aviation. As AI in aviation has a direct implication for aviation safety, this agency develops standards and recommended practices, procedures, and guidance material to be used by member states to enable a global effective and harmonized implementation of safety measures.

A regulatory product impact assessment of advanced AI in aviation revealed a strategic priority to shape the standards and recommended practices on AI, which further refers to a joint effort concerning commercial aircraft certification.

Among the many challenges, issues such as jurisdiction, accountability, and in general the enforceability of new AI regulations could slow down the regulatory action of the aviation authorities. But the implementation of the services in the end would make it faster and even safer. There is no mention regarding how, aviation authorities will enforce compliance with these measures. At the same time, the paper contends that the role of the authority is indeed instrumental in the aviation safety regulation of AI and automated vehicles. Continuous monitoring is necessary to detect problems with AI and intervene promptly for corrective purposes. This begs questions, should standards and recommended practices be inversely developed taking into account the level of technological development to establish certain theoretical requirements, including the human-factor? In this case, global aviation safety will require the introduction of standards for civil aviation to ensure the coordination and understanding of measures corresponding to the readiness of the individual states. However, it must be acknowledged that there are currently no aviation agreements concerning the mutual recognition of pilot competencies, which limits the practical performance of functions in another country. This also prevents providing for a management system with different automated systems between nations of varied technologies.

LIABILITY AND ACCOUNTABILITY IN AI AVIATION SYSTEMS

As AI systems are introduced into aviation, questions about liability and accountability may emerge, including who is liable for the actions of AI systems when failures occur. It can be expected that introducing AI will alter or complicate traditional aviation liability paradigms, including concepts of strict products liability for manufacturers who sell airplanes, which are not usually thought of as being

"defective" in the sense of a product causing personal injury. Illustrative questions are: (1) Who may be at fault when an AI system fails to meet a reasonable standard of care? (2) How do we prove it acted negligently or in a way that falls below ordinary care? (3) Does it matter whether or not an AI system is "ultra-high-fidelity"? (4) What standards of care credit should be assigned to human operators and AI systems, and what percentage of each would be necessary to avoid liability in operational failures? (5) How does this interrelate with the need for developing a proactive safety culture that replaces a reactive blame culture?

Legal principles that may guide liability for AI in aviation include standard principles of tort law and product liability, as well as agency law and antitrust law. The law principally directs inquiry to liability and away from regulation. One can see this in the discussion of tort liability considerations on AI. In discussions of AI in other critical sectors, scholars and policymakers have shown thoughtful prudence, acknowledging the risks that newly introduced technologies will have in large-scale harm events. Scholars have noted that AI may change how we allocate legal burdens, and in courts of law, jurors who adjudicate blame can struggle with unexplainable AI decisions. Comparative observations from liability gaps may be instructive. For example, the literature points out that data spans beyond national borders and that a possible gap could arise in assigning liability when data is combined to train AI from different countries. Moreover, case law points to potential gaps in applying existing doctrines of causation, including in the application of legal causation principles and the unit of liability in propositional machine learning. Cutting across laws and jurisdictions, work has elaborated on legal and ethical considerations for accountability, while consideration has been given to liability in the introduction of unmanned aircraft, focusing also on the importance of public trust. The foundation of international aviation law segregates liability and safety. Not unlike other sectors of international law, this framework is based on an agreement that bureaucrats should operate without fear of tort liability

However, tools like the Aviation System Oversight Program signal a growing understanding that individuals do not operate aircraft in vacuums and should not be seamlessly segregated where they are part of a system. This is particularly pertinent where an AI-dominated flight deck is being integrated into an existing system that has liability regimes in place.

Legal Principles of Liability

In this subsection, we briefly explore the legal principles of liability and discuss whether and, if necessary, how these general principles should be modified to fit AI technologies, specifically AI for aviation. The principles of liability remain the basis for any legal order, including the question of liability in the context of AI. Legal traditions recognize different concepts of liability, such as contractual, non-contractual, and other liability regimes like liability for ultrahazardous activities and compensation for fault-based defects in the legal process.

In the aviation domain, liability questions with respect to AI can mostly be traced back to either the negligence of the AI developer, the manufacturer, or the human system designer, the air operator, etc. There is also strict liability, liability without fault; a further development of such liability is safety liability. Finally, historical principles or assumptions on accountability, such as vicarious liability and

respondent superior, are being discussed with respect to AI. These legal principles apply more or less to AI as well, but of course, the characteristics of machine learning, for instance, require a specifically adapted understanding of each of these. If we look at the situation in the aviation domain, the question arises whether our principles of liability are sufficient to cover the cases concerned with AI. The legal regime of liability cannot cope with AI technology. One argument for this position concerns the increasing autonomy that is connected to machine learning: AI will develop and apply its own courses of action and strategies in the face of unforeseen events in a way that human operators do not comprehend and do not even foresee.

Abandoning such an approach and sticking to traditional concepts would imply closing our eyes to those operational contexts of AI application that heavily rely on machine learning, thus limiting its deployment. AI running on machine learning, due to humanly unforeseeable action strategies of its own, represents the greatest challenge for liability. Several case studies are mentioned where human operators lost track of what their algorithms are doing and how they reach decisional conclusions. This is particularly the case for data-driven AI.

DATA PROTECTION AND PRIVACY CONCERNS

AI is likely to generate significant concerns regarding privacy and data minimization, mainly due to its need for a large amount of data to learn and train itself. The fact that new solutions seem to be mainly functioning based on the collection, storage, and further processing of personal data brings a range of compliance challenges.

In light of the massive amount of personal data stored by aviation stakeholders, the sector raises concerns about the possibility of machines inadvertently making protected data public. Such fears are particularly pronounced following the failure of airlines to safeguard their customer data. The sheer size of these pools of data suggests that data breaches involving biology are no longer laughable – samples handled by new software could now comprise thousands of individuals, opening the door for large-scale data harvesting. A recurrent thread running through the AI narrative, therefore, concerns itself with the implications of the technology for passengers in terms of data protection, surveillance, and privacy. In short, the idea of availing oneself of an AI-powered or drone service opens passengers up to a host of data protection risks. The gravity of these risks is further amplified by the strict provisions applied across the EU under the General Data Protection Regulation. Due to the heavy penalties imposed, airlines are understandably anxious to ensure they are not only compliant but also seen to be compliant. With so much at stake, one might expect airlines to take more robust forms of verification and proof by adopting the reverse burden of production. All considered, there appears to be a well-trodden path towards a harmonious relationship between AI technology and rules, etiquette, and ethics. Given this, current political challenges associated with the implementation of AI technologies in aviation seem to arise rather from a lack of information among the traveling public, or at least among segments thereof. Thus, a number of low-level daily struggles and objections have emerged, focusing on privacy and the data protection potential that AI technology raises for citizens.

GDPR Compliance in Aviation

Given the amount of passenger information that is being stored, whether for just the time of the flight or longer, it is important to ensure that this is carried out correctly. The regulation holds a number of principles that all data users within the European Union must adhere to. The first is that processing should be lawful, fair, and transparent. In AI, this means that any passenger data that is collected, used, or stored must be done so legally. This means either that the passenger has given clear consent for this action, that the action meets the need to process for a contract that is being engaged in, or that there is a regulatory requirement for this to occur.

The data that is collected by AI must also be used for the purpose for which it was collected. In aviation, this means providing services such as booking, baggage carriage, flight safety, and medical information. In general, AI may collect more information to improve customer service, sales, or operations. The data obtained should be relevant and not excessive, and passengers should be told how long it will be stored, as it should not be held longer than what is needed. This includes the passenger having a right to ask for their data to be deleted. This also includes ensuring that the data is accurate and up to date. Where there are concerns that larger AI systems will struggle with assessments, versions specifically looking for bias in AI have been suggested as a way to lower the time and economic costs to the company.

The risks can be reduced by controlling who has access to the data and maintaining confidentiality. In practice, many existing operations can be updated, and an organization can use privacy by design methodology to ensure that the whole organization is aligned for these privacy changes. Similarly, non-identified identifiers or anonymization strategies can be used for data to ensure its isolation, preventing individuals from being specifically identified. This requires a company to use sufficiently strong protection mechanisms; however, otherwise, the controller will still be liable should this be compromised.

Ethical Considerations in AI Aviation Systems

As AI systems are intended to operate in real environments, a lot of attention is given to establishing a set of ethical guidelines to ensure that data science and AI technologies are used for the public good and that trust in them is maintained. While it is logical to look closely at established benefits and risks of AI systems in healthcare and social welfare, these should also be investigated in aviation, where the benefits of AI implementation are predicted to be significant. The safety and efficiency of AI systems should be balanced together due to the fact that benefits and risk trade-offs do exist. The transparent, explainable, accountable, and fair AI applications bring great benefits to the aviation industry, but, on the other hand, may slow the introduction of new functionalities and applications. A comprehensive decision-making process involving the alignment of different ethical principles in AI is required between the social desirability and technical possibility of a solution.

Given the recent ethical controversies on data processing, it is highly relevant, although speculative because new data are due, to report on how various approaches can be used for identifying meaningful dilemmas, which require explanation at several levels. Dilemmas are considered at the level of function with special focus on the relationship between AI and pilots and within the safety culture dimension while paying attention to the process-oriented perspective. Given the recent ethical controversies on

data processing, it is highly relevant, although speculative because new data are due, to report on how various approaches can be used for identifying meaningful dilemmas, which require explanation at several levels. Dilemmas are considered at the level of function with special focus on the relationship between AI and pilots and within the safety culture dimension while paying attention to the process-oriented perspective.

A study group report also proposes a draft code of conduct. It currently addresses professionals connected to AI technology, and companies that manufacture, repair, overhaul, or use systems containing AI technology. Despite these efforts, more regulations will be necessary to take into account new types of technologies and their ramifications.

CASE STUDIES AND LEGAL ANALYSIS

So far, the usage of AI in aviation has been similar to how Airlines envisage and use Data Analytics. Dynamic pricing is an aspect for which AI is known for being used by the Airlines, Lufthansa, Emirates and Southwest, apart from these major operators there are some small-time operators as well that use AI augmented predictive systems for multiple reasons.

It was laid down in the case of *Max Schrems v. Facebook Ireland Ltd* the usage of user generated data for the purposes of analysis do raise data rights related concerns and as per EUGDPR if it is at all used for a purpose not specified prior leads to the violation of the EUGDPR.

Furthermore, from the case of *United Airlines v. Department of Transportation* on the issue of Algorithmic Bias and Discrimination, it can be stated that algorithms perpetuate existing biases in the interpretation of data, and even in AI augmented models it has been observed to persist. This often leads to discriminatory pricing, or impact services in a discriminatory manner including boarding and security screening and etc.

Determination of legal responsibility for accidents is prior or presumptive concern for usage of AI in Aviation, as the liability regimes aren't defined or properly laid down yet, from the case of *Google v. Waymo*, it can be stated that every case leads to a conflict of liability amongst the manufacturer, operator and even the AI itself. As such, as this is still an emerging are, the ICAO is working on the regulation focusing on harmonization attempts at regional BIT models and Multilateral agreements as well.

FUTURE TRENDS AND CHALLENGES IN AI AVIATION

The future trends indicate an increasing integration of AI technologies into the aviation sector. The development of advanced analytics of big data extracted from a plurality of operations enables the augmentation of human ability in performing decision-making processes. Also, the introduction of algorithms strongly based on a machine learning approach can be adopted in the aeronautic scenario. In addition, as a direct evolution of machine learning techniques, one of the most relevant challenges of current aviation is digitalization, regarded as the introduction of autonomous systems and the redesign of current systems in order to safely introduce this enhancing technology in the aviation market. These advancements lead to a growing potential of using AI and related tools or techniques in aviation for the implementation of autonomous aircraft able to make their own decisions based on

acquired data. Implementing AI and autonomous systems will introduce various benefits for aviation, such as cost reduction, flexibility in carrying out operations, limiting human errors, and potentially significantly increasing safety.

At the same time, these advancements will introduce different facets to be carefully covered in a legal framework, for example ensuring that no ethical considerations are violated, or obligations related to the explainability and the level of trust in AI utilized. Other emerging challenges relate to the continuous maturity of AI capabilities that will be needed both in the design of suitable training tools and in the monitoring of their proper use. Also, the adaptation of current regulations to AI capabilities in air traffic management and systems will be an arising issue in the future. Legal frameworks are likely to establish ideals while empowering international and national authorities and industry players with the mandate, capacity, and tools to develop practices adapted to the nature of the emerging technologies. They do, however, carry the potential for lack of agility if they are only adjusted through formal channels. A cooperative and efficient process to manage this complexity and ground the high-level guidelines into practical requirements will be needed between various industry stakeholders and creative authorities looking to safely support innovation. This changing landscape supports the call for further research in the field. Up-to-date analysis of how AI is integrated into aviation will allow better monitoring of aviation system safety aspects and timely adaptation of existing practices. Also, the increasing ability to autonomously analyse big data regarding hazardous situations and the new normal will not only enable predictive and seamless adaptation of monitoring and enforcement but also enhance the safety case. Synergies and possible conflicts considering AI in the different domains will have to be addressed by the authorities and industry in a cooperative manner, enabling proper technology evolution and the reduction of synergistic and discriminatory risks.

Commercial deep learning-based systems have gained traction in many applications that require people to analyse and predict asset prices, government policies, and other areas motivated by properties of the training data. Examples of this that have particular relevance for aviation include predicting maintenance schedules based on engine and aircraft data, predicting wind shear and turbulence for pilot assistance and flight planning, predicting touchdown deceleration for aircraft pavement loading and approach control, traffic route optimization to reduce airspace congestion and improve security, foreign-object debris detection and reduction, automation of air traffic control, and a more realistic and flexible simulation for pilot training and entertainment. As a result, deep learning has the potential to introduce new research avenues and should be understood and applied to improve aircraft safety, comfort, efficiency, and capacity worldwide.

The various applications of these robotic systems address the issue of the conduct of remotely operated and autonomous systems in the common domain, i.e., the airspace and the right to access from one state to another. This has significant ethical and legal implications that must be addressed, such as rights to privacy and end users' authority to opt out of data sharing in countries such as the EU Member States. This highlights a primary focus on governance and political economy issues and how shaping policy can unlock technological, economic, and social development potential by driving technology deployment at scale in a privacy-compliant and democratically legitimized manner. It also reinforces

the caution supported by regulators in heavily regulated industries who have noted that algorithmic decision-making technologies are relatively immature and any use of the uncertainties can be very high. The speed at which technology is advancing significantly in comparison to enacted legal measures poses a core issue for both generalist and specialist regulators.

CONCLUSION AND RECOMMENDATIONS

This study has shown that the development of AI technologies has begun to change the field of aviation law. The most critical challenge is to develop solutions based on existing legal frameworks. Besides, the moral and ethical aspects of AI and the legacies of the ultimate step for safety and the identification of responsible parties increase the risk of damage. Based on the analysis of the relevant aviation laws it can be concluded that the way forward is to develop recommendations that can be adopted by authorities and stakeholders regarding the use of AI technologies. Accordingly, the first recommendation suggests that legal technologists, legal experts, authorities, and stakeholders from throughout the aviation value chain should be working proactively to ensure that a legal framework governing the area of AI technologies can be implemented effectively. To develop policy and legal norms, regulatory impact assessment should be prepared. It is also recommended to include all stakeholders in the regulatory process. A regulatory committee should be established on issues where different opinions can be expressed.

For the implementation of AI in aviation, the harmonization of International Law is of paramount importance, uniformity in model BITs and MAs, facilitated by the International Investment Law are a key to it. Furthermore, to dilute AI related liability dilemmas and diminish the risk of failures, there should be human supervision on every task that has been automated by the usage of AI.

*****

CYBERCRIME AGAINST WOMEN IN INDIA: A COMPARATIVE STUDY OF PRE- AND POST-COVID-19 PANDEMIC PERIOD

Dr. Ramesh Chandra Sethi[43] and Arpita Jena[44]

ABSTRACT

Background: The COVID-19 pandemic has created havoc in all Nation-States worldwide. The transmission of the virus led to an increase in cases that led to the global imposition of lockdown. This situation forced a large number of people confined within four walls, including women, to be engaged in surfing the internet (i.e., the use of the internet and various social media platforms) during the pandemic. As stated by the National Crime Records Bureau (NCRB), the Government of India, there is an increasing number of cybercrime cases against women from 8,415 (2019) to 10,405 (2020), and it further jumped to 10,730 cases in 2021 during COVID-19. It indicates that heavy browsing of the internet led to a significant increase in Cybercrimes Against Women (CAW) during the pandemic.

Objectives: (i). To critically analyze the root causes of cybercrimes against women in India; (ii) To scrutinize various judicial pronouncements related to CAW. (ii). To critically investigate and examine the data published by the National Commission for Women (NCW) and to find out the trends of CAW in India before and after the pandemic.

Methodology: This study is based on doctrinal research of secondary data sources followed by qualitative and quantitative research methods.

Findings: The findings suggest that the imposition of lockdown has increased CAW due to their active engagement in the digital world. The study also reveals that educated, tech-savvy women living in cities are more prone to victims of cybercrimes.

Conclusion: India has adopted various stringent laws to prevent cybercrimes. However, due to a lack of awareness, effective and efficient rule implementation, and robust monitoring mechanisms, the government has failed to ensure a crime-free society for women even after 78 years of independence.

Keywords: COVID-19 pandemic, women, cybercrime, technology and legislation.

INTRODUCTION

The 'COVID-19' had a profound effect on all facets of life. To tackle its spread, the government of India had enforced a complete lockdown measure across the country. As a result, people are confined within four walls without any work. The isolated life with no work and other engagement has forced people, specifically young women, to surf the internet (i.e., the use of the internet for different purposes, including online shopping and use of various social media platforms) during the pandemic. The large volume of internet users ultimately falls into the trap of 'cybercrime' (Mondal and Paul, 2022). The victims of this crime are mainly women because there is a growing number of women who depend on online sources for a variety of purposes, which include employment, education, purchasing goods and availing services, personal and social contacts, entertainment, and related operations etc. The more time they spend on the internet, the probability of more cyber fraud they face, and the offenders get more

[43] Assistant Professor at School of Law, Kalinga Institute of Industrial Technology (KIIT), India.
[44] Student at School of Law, Kalinga Institute of Industrial Technology (KIIT), India.

opportunities for committing cybercrime. According to UN Women's research, the global surge in internet use throughout the 2020 pandemic has led to a spike in reports of virtual abuse against women. It was mentioned that as women spend most of their time virtually so, there is a higher chance of experiencing virtual harm, such as threatening and defamatory content, as well as sexual abuse messages and sexual violence, which ultimately leads to an increase in cybercrime. Therefore, the UN has termed the 2020 pandemic a 'Shadow Pandemic'.

Furthermore, 'Online Gender-based violence against women (Online GBVAW) is defined as any act of GBVAW that is committed, assisted or aggravated in part or fully by the use of information and communication technologies (ICTs) such as smartphones, internet, social media platforms or email, against a woman which led to the growth of crime against them disproportionately.' When it comes to a spectrum of various, recurrent, and connected types of violence based on gender, it was found that women experience more virtual abuse than men while accessing the internet. Social networking sites should not be a place of safety and security for women, though they have become essential to their lives in this digital age. Women often self-censor in response to online harassment they face, either by stopping the use of social media altogether or drastically cutting back without going and reporting the incident to an appropriate authority. This simply highlights the fact that women cannot exercise their Constitutional rights to 'freedom of expression and a dignified life,' as stated in 'Articles 19 and Article 21' of the Indian Constitution. It was further observed that the psychological effects of online harassment are severe, and women feel insecure utilizing cyberspace. They also hesitate to get legal support because of insecurity and societal stigma. As per the data of the UN, it was observed only 10% of the women who were victims registered their complaints at the police station. In contrast, 90% of women still hesitate to take legal protection due to societal stigma and personal dignity.

Further, as per the National Crime Bureau Report (NCBR, 2020), it was held that there is a 24% decrease in all crimes related to women, but simultaneously, there is a 54% increase in cybercrime among women. These data showed that the rise in dependency on the internet led to a severe increase in cybercrime against women. Though the Parliament of India has made thousands of laws for protecting women, their negligence of not disclosing the cases/crimes has led them to be more prone to cybercrime. To reduce cybercrime, there is a need for adequate awareness and combining efforts along with stringent laws to fight against cybercrime, making India a better place for the safety and security of women.

METHODOLOGY

This study is qualitative doctrinal research. The data are collected from various secondary sources, and other relevant information is available in multiple publications, documents, and reports of the Government of India and national and international institutions/ organizations. Furthermore, the study analyzes the trends of increasing cybercrime, as per the data given by NCBR and the analysis of data provided by each State regarding various cybercrimes against women.

CAUSES FOR CYBERCRIMES

(i) Judicial reasons

The preamble of the IT Act of 2000 shows its primary goal is to enhance e-commerce. Enhancing e-commerce encompasses business and economic offenses such as fraudulent activity, violation of confidentiality, and malware that steals confidential information. The S.66,67,72 of the IT ACT, 2000 deal with these things. These three sections deal with everything except e-commerce offenses. Whereas there is an increase in the number of crimes related to women, like cyberbullying, cybersex, etc., that are not dealt with specifically under the IT Act, the IPC and the Indian Constitution give protection against crimes such as rape. Outraging the modesty of women, they also fail explicitly to provide security to women related to cybercrime. Following the '2012 Delhi gang rape case (Nirbhaya Case)', there has been a significant public uproar calling for new laws and regulations to be implemented to safeguard women from criminals. 'Sections 354, 354 A, 354 B, 354 C, and 354 D' are among the changes to the IPC made possible by the 2013 Criminal Law Amendment Ordinance.

(ii) Societal reasons

The majority of cybercrime increases because the victim hesitates to disclose the crime as she fears her family's reputation will be damaged. She firmly believes that she will be blamed and her dignity will be destroyed in society. As a result, she does not disclose the crimes committed to her. Women are more susceptible to cybercrime because the criminal's identity is unknown, and he may use fake identities and persistent threats to harass the victim. Women are worried that coming forward with the crime and complaining in an appropriate forum might make lives more difficult. They are also in a dilemma, whether their friends and relatives will stand by and support them or not. They are also worried about the effect the after-event will have on society. Owing to these anxieties, women frequently neglect to report crimes, which raises the morale of those who commit them and increases cybercrime significantly in India.

(iii) Easy accessibility by the perpetrator

When we discuss crimes, we typically consider aggressive offenses involving bodily harm/injury. To commit such crimes, we often need to perform some physical labor and create a plan to carry out such action with a weapon. However, that is the opposite when it comes to cybercrime. In this case, a person can be a perpetrator by simple devices in the modern world. Cybercrime can occur anywhere without a territorial nexus, making it much easier to commit than other physical crimes.

(iv) Increase of male users in social media as compared to females

Research states that most internet users are male on any social networking platform. As per the data of the IT Department, it was found that around 73% of users are male compared to females. This can be another reason why women are the target when a large number of male members are on these platforms, as they strictly go by the patriarchal mindset. Even today, many male members think women should not be using social media sites. Hence, this notion of patriarchy may lead to several agonies, which ultimately results in cybercrime.

JUDICIAL PRONOUNCEMENT

(i) "Manish Kathria v. Ritu Kohli" - is the first related cyberstalking case. In this instance, Mrs. Ritu Kohli reported to the police that someone had been employing her personal information to speak online at 'http://www.micro.com/,' primarily in Delhi. The police looked into the case in detail and apprehended the perpetrator. Further, the individual used her identity, provided her address, and engaged in vulgar behavior when communicating online. Additionally, the same individual purposefully provided other participants with her phone number, urging them to give her a call at additional hours. As a result, she received nearly 40 calls in three days during the additional hours. These calls created an agony in her private life. Furthermore, the IP access of the culprit was found by the police, and then the culprit was arrested. Subsequently, the case was registered, but unfortunately, the culprit was bailed and released. The cyber laws in India do not address cyberstalking. The only area where an individual can be charged remotely for violating privacy and secrecy under Section 72 of the IT Act. The culprit could be additionally charged under Section 441 of the IPC and Section 509 of the IPC.

(ii) "State of Tamil Nadu v. Suhas Katti": In this case, the accused person created a fictitious e-mail ID of the victim's identity and forwarded communications to the divorced woman to obtain details. The victim experienced psychological assault as a result of the publication of comments as she continues to receive bothersome phone calls. As a result, in February 2004, she complained to the Egmore Court and the Cyber Unit of the Tamil Nadu Government. The Cyber Unit took the accused person into custody. He was charged under Sections 67 of the IT Act of 2000 and 469/509 IPC after proving that he had committed an offense.

(iii) "Avnish Bajaj v State of (N.C.T) of Delhi": A customer-to-customer company called Bazee.com was discovered to be selling MMS recordings under the guise of "DPS girls having fun." The chief executive officer of the sales company, Avnish Bajaj, was detained, and his request for release was denied. The IT Act of 2000's section 67 led to his detention. The defendants in the present instance argued that section 67 of the Act deals with the printing and distribution of pornographic material rather than its delivery. The court ruled that the real pornographic video or clip could not be viewed on the Baazee.com platform. The court granted the offender bail alongside a one lakh surety.

COMPARATIVE SCENARIO OF CAW IN PRE- AND POST-COVID PANDEMIC PERIOD

Table-1 and Figure-1 (given below) show the crime against women before, during, and after COVID-19 from 2018-2023. It was observed that 49953 CAW were committed in the last five years (2018-2023), out of which 6030 crimes were registered in 2018-2019, followed by 8379 cases in 2019-2020, and in 2020-2021, there was a sudden 20% (10405 cases) increase in CAW due to the complete lockdown and all including women were confined within four walls and ordered all essential commodities from the online sources for their day-to-day activities. Therefore, women are more vulnerable to cybercrime. Furthermore, the lockdown boosted the number of individuals meeting online, which has raised the prevalence of online pornography to 1655 in 2020-2021 from 1174 in 2019-2020, and digital stalking increased to 887 in 2020-2021 from 785 in 2019-2020. Similarly, other types of cybercrimes, namely morphing (251 cases), cloned profile (354 cases), and other crimes (7184 cases

in 2020-2021 from 5995 in 2019-2020) against women also increased significantly (see Table-1) during 2020-2021 post COVID-19 pandemic period. This happened because of the absence of knowledge of legal procedures, lack of consciousness, and inadequate cybersecurity protections, which led to women being targeted by hackers. The majority of perpetrators of cybercrime are women, which has been sharply increasing day by day. The COVID-19 shutdown has contributed to a boost in cybercrime incidences nationwide. About 10,405 CAW cases were formally recorded in 2020-2021, per the (NCBR). Table-2 shows that around 49953 cybercrimes were committed against women between last five years from 2018 to 2023. In 2022-2023, around 27.09% of cybercrimes against women were committed in Karnataka, compared to 22.07% in 2018-2019. This trend shows a 3% increase in cybercrime, making Karnataka a more prone State to CAW. So, the State of Karnataka recorded the highest number (13078 cases in Karnataka alone) of CAW followed by Maharashtra (8624 cases), Assam (3910 cases), Uttar Pradesh (3666 cases), Telangana (3418 cases) and Odisha (2373 cases) in the country. Besides analyzing data, CAW in India continues to be overlooked as a serious issue. Typical internet extortion techniques being used against women include objectification, defamation, picture morphing, harassment, and demanding cash as compensation for sating sexual desires. Women's confidence in utilizing networking sites and the World Wide Web has also been damaged, and there is now a real risk to their safety and anonymity. Hence, it can be concluded that women are more prone to cybercrime. While it is evident that ever since the pandemic in India, cybercrime has caused considerable harm, various reasons have exacerbated the problem and increased cybercrime cases. Undoubtedly, the internet has benefited human civilization in many ways, but simultaneously, it also causes harm to society at large.

Table-1: Types of Cybercrime Against Women

Types of cybercrime	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	Total
Threatening	113	132	74	200	125	644
Pornography	862	1174	1655	1896	2251	7836
Stalking	738	785	887	1172	1457	5039
Morphing	62	65	251	276	385	1039
Cloned profile	207	288	354	225	179	1253
Other crimes	4048	5995	7184	6961	9870	34058
Total cybercrime against women	6030	8379	10405	10730	14409	49953

Source: Crime Report 2018 to 2023, NCBR, New Delhi

Figure-1: Types of Cybercrime Against Women

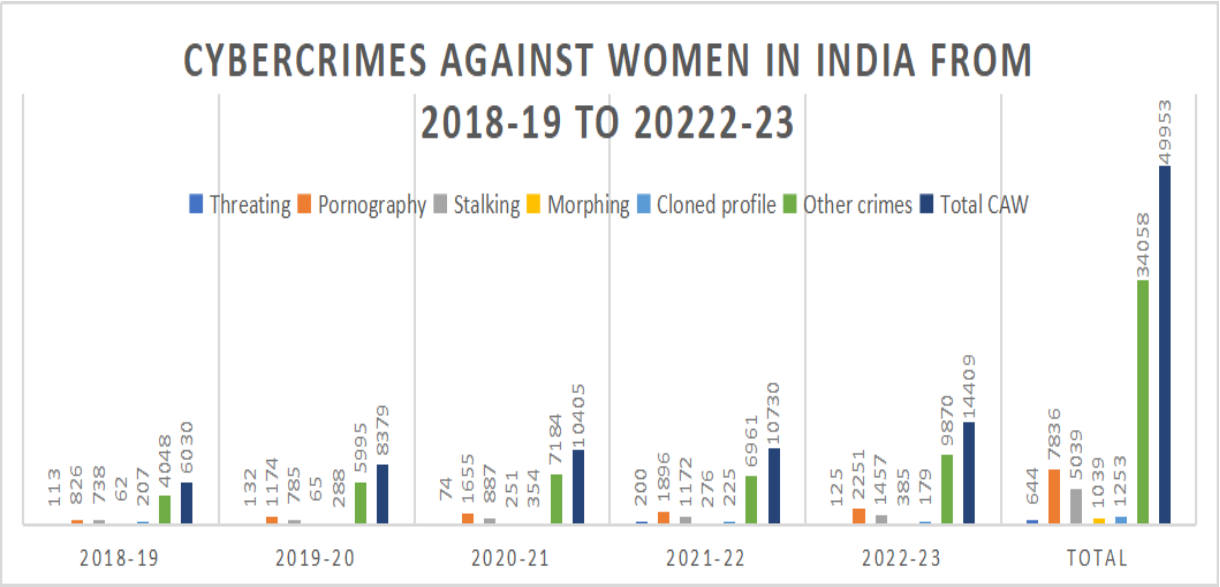


Figure-2: State-wise Cases of Cybercrime Against Women in India

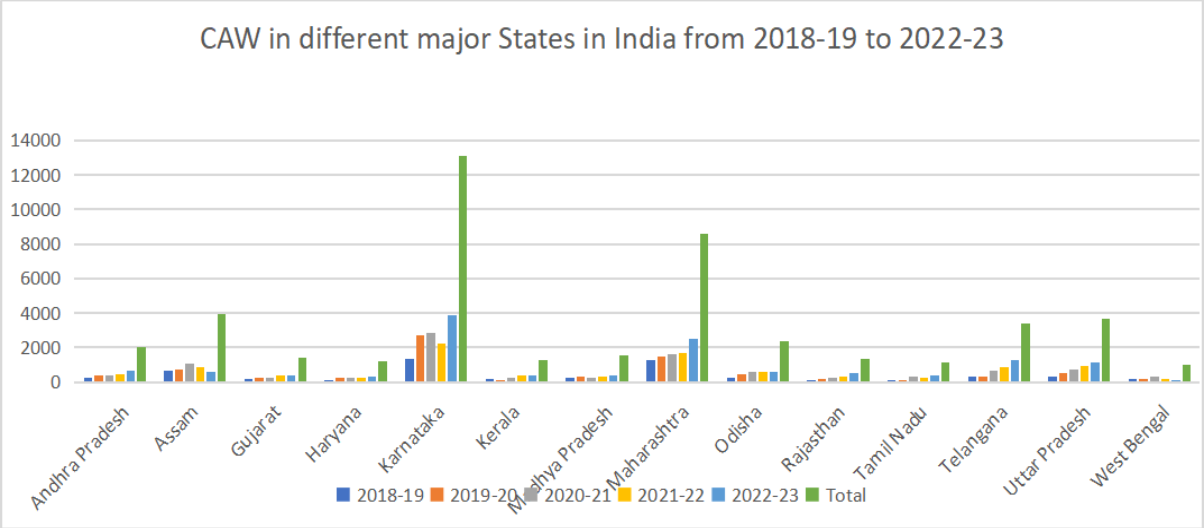


Table-2: State-wise Cases of Cybercrime Against Women in India

State/ UT	2018-19	2019-2020	2020-2021	2021-2022	2022-23	Total
Andhra Pradesh	217	356	375	471	637	2056
Arunachal Pradesh	1	5	1	16	5	28
Assam	670	703	1071	856	610	3910
Bihar	14	60	47	56	84	261
Chhattisgarh	64	85	117	194	279	739
Goa	21	5	19	15	32	92
Gujarat	184	226	277	349	352	1388

Haryana	112	251	222	266	327	1178
Himachal Pradesh	52	47	52	39	46	236
Jharkhand	13	43	20	70	106	252
Karnataka	1374	2698	2859	2243	3904	13078
Kerala	160	139	246	353	381	1279
Madhya Pradesh	276	301	274	298	390	1539
Maharashtra	1262	1503	1632	1697	2530	8624
Manipur	9	2	26	39	13	89
Meghalaya	32	21	39	21	27	140
Mizoram	4	2	1	13	0	20
Nagaland	2	1	2	1	1	7
Odisha	228	437	560	574	574	2373
Punjab	97	87	110	179	194	667
Rajasthan	116	188	238	297	498	1337
Sikkim	1	1	0	0	11	13
Tamil Nadu	77	124	306	248	401	1156
Telangana	336	288	649	883	1262	3418
Tripura	5	3	3	1	4	16
Uttar Pradesh	340	518	749	958	1101	3666
Uttarakhand	78	28	72	183	161	522
West Bengal	170	170	344	201	142	1027
A&N Islands	5	2	3	3	12	25
Chandigarh	5	13	10	12	16	56
D & N Haveli	0	2	3	2	2	9
Daman & Diu	1	0	2	2	3	8
Delhi	79	56	51	151	250	587
Jammu & Kashmir	23	14	25	39	39	140
Lakshadweep	3	0	2	0	0	2
Puducherry	0	0	0	0	15	15
Total	6030	8379	10405	10730	14409	49953

Source: Crime Report 2018 to 2023, NCBR, New Delhi

CONCLUSION

In India, women's safety and security has been neglected due to the patriarchal nature of the society. At the same time, there is lack awareness for legal entitlements and women empowerment. All forms of crimes against women are on the rise, but becoming a target of cybercrime is perhaps the most painful experience for a woman. It is not only highly prevalent in India but also around the world. During the outbreak of 2020 COVID-19 pandemic, more women are forced to use the services of the internet and it resulted in the effects on their emotional, interpersonal, and physical wellness as well as a higher likelihood of digital bullying and intimidation of the victims. The pandemic was a period when women were more vulnerable to cyberbullying due to their growing reliance on electronics gadgets. It also highlighted the need to foster an atmosphere of distrust to avoid the abuse of information and data privacy. Although, India has implemented IT Act, 2000 to combat cybercrime but this IT Act has not successfully addressed the critical issues pertaining to the privacy and protection of women. The majority of instances of cybercrime remains unreported because Indian women are either ignorant of it or afraid of it. This kind of ignorant and soft attitude provide opportunities to the criminals to go away after committing the cybercrime. Many private and public websites and other online platforms offer security advice for women's online safety. Hence, proper awareness along with combining effort and strict implementation of laws specifically dealing CAW can help in combating CAW and to make India a better place for women's safety, security and provide a sustainable world for the women.

*****

REFERENCES

- Rathor and Das, "Cyber Crime: The Emerging trends and challenges", CyberSpace and Law : Issues and Challenges, NALSAR University, Hyderabad, 2004 p. 102.
- Snook A., "Stalking in the workplace the complete guide to prevention and investigation", available at: https://www.i-sight.com/resources/stalking-in-the-workplace-the-complete-guide-to-prevention-and-investigation
- Dr. Mrs. K. Sita Manikyam, Cyber Crime – Law and Policy perspectives, 40 (Hind Law House, Pune, 2009).
- Cyber Crimes and the law, Legal India,legalnews and law resource portal (Mar 30,2024,03:21 PM), available at http://www.legalidia.com/cyber-crimes-and-the-law/.

*****

THE GEOPOLITICAL CHESSBOARD: AI AS THE NEW WEAPON IN THE ARMS RACE

Shrishti Shrivas[45] and Diksha Tripathi[46]

ABSTRACT

The rapid advancement in AI has ushered in a new arms race among major powers that has substantially changed global security dynamics. The research explores the integration of AI into military devices, which transforms modern warfare as well as strategy to nations' security. Given the rise of an AI supremacy race among the powerful countries, including the "United States, China, and Russia," what was once considered a destabilizing power transition is becoming too apparent not to be put under the spotlight. Military integration of AI into the system raises quite serious legal and ethical issues that need consideration right away. This research also addresses issues such as accountability, autonomous decision-making, as well as a lack of broad international collaboration. The entry of private tech corporations into the battle for military AI technology further complicates an already complex geopolitical situation. The authors of the study are greatly interested in international tandem for developing an ethical and legal configuration to ensure AI improves global security while ensuring human rights and ethical norms.

Keywords: Artificial Intelligence (AI), Global Security, Ethical Concerns, Legal Implication, International Cooperation

INTRODUCTION

The quick rise in the usage of artificial intelligence (AI) has resulted in an extraordinary shift in global security and defense strategies, adding new dimensions to military systems and technology. What was once science fiction has become a reality, with powerful nation such as the "United States, China, and Russia" at the forefront of this emerging arms race, competing not only for military superiority but also for leadership in usage of AI. This race has generated significant changes in global security dynamics, altering current war plans and state defense postures across the world.

The capacity of artificial intelligence to improve predictive analytics, process enormous amounts of data, and enable autonomous decision-making systems is changing the way wars are fought.From combat drone automation to the building"of autonomous weapons systems, artificial intelligence"has evolved from conventional support roles to the forefront of military operations.

The focus of the paper is majorly inclined towards examining the multifaceted implications of artificial intelligence in military applications, leading to a new race among the nation for developing AI powered weapon, along with developing of the need for rethinking of international legal frameworksin a way that prioritizes global security and human rights. Further the paper also deals with the position of the private tech companies involved in the growing development of AI. Therefore in an era where technical improvements outpace regulatory restrictions, understanding the geopolitical implications of AI as a new weapon in the arms race is critical.

[45] Student at Narsee Monjee Institute of Management Studies, India.
[46] Student at Narsee Monjee Institute of Management Studies, India.

STATEMENT OF PROBLEM

Through military arms, AI has accidentally augmented the rivalry across the globe. All powers would love to have their contribution as the major destination for AI. With appropriate guidelines and regulations across international borders, these perils may expand without any limitations. Therefore, it is genuinely important to regulate AI sensibly in military arms without aggravating any war in the future and to maintain world peace.

RESEARCH METHODOLOGY

This research work is going to be conducted through qualitative research methodology, applying data sources which are secondary most of the time in the analysis on the effects of artificial intelligence over military conflicts and global security. Information is gathered from diverse official reports, scholarly journals, and other reliable online sources that have an effectiveness aimed at proving valid and reliable data. Themes key include technological advancements, ethical challenges, and international regulations.

THE GLOBAL AI ARMS RACE

With major international powers competing for dominance in military artificial intelligence technologies, the ongoing AI arms race represents a watershed moment in the evolution of modern warfare. Leading governments, “including the United States, China, Russia, and” others, havee greatly increased financing for artificial intelligence research and military applications. Their activities not only challenge military doctrine, but also raise moral, political, and legal concerns. This section delves into each country's individual efforts, to show the vital role AI plays in international power relations.

- **United States: AI and Defense Innovation**

“As seen by initiatives like Project Maven and the establishment of the Joint Artificial Intelligence Center, the US Department of Defense (DoD) has been a pioneer in the use of AI technologies.” The 2020 Congressional Research Service study states that since 2017, the US has spent over $18 billion on defense research pertaining to AI, with uses ranging from AI-assisted cyber defenses to autonomous drones.

As an illustration, consider DARPA's "AI Next" initiative, which aims to incorporate AI into intelligence, “surveillance, and reconnaissance”(ISR) missions as well as other military systems. Additionally, the US is “at the forefront of the invention” of “Lethal Autonomous” Weapon Systems (LAWS), that has raised questions regarding the morality of autonomous combat. Although this places the US at the forefront, it has also spurred a race for weapons in which other nations have responded in kind.

- **China’s Pursuit of AI Supremacy**

China's "Next Generation Artificial Intelligence Development Plan" outlines “its intention to be the world leader” in AI by 2030. According to a Brookings Institution analysis from 2021, China's yearly AI defense spending is anticipated to be $2.7 billion, ranking second only to the United States. China

has concentrated on creating AI systems that improve cyber capabilities, ISR technology, and self-driving combat vehicles.

China's employment of AI-powered surveillance systems, both domestically and globally, reveals the dual purpose of its AI capabilities. For example, the use of AI facial recognition systems in Xinjiang for mass surveillance has sparked global outrage, underscoring the ethical difficulties involved with China's AI uses in both military and civilian settings. Furthermore, China's engagement with private businesses such as Huawei and ZTE accelerates its technological growth, opening up new possibilities in cyber warfare and digital espionage.

- **Russia: Strategic deterrence and AI**

Russia's AI military spending, are increasingly focused upon strategic deterrence. Russian Ministry of Defense has identified artificial intelligence (AI) as crucial to future combat systems, including autonomous weaponry such as the Uran-9 unmanned combat vehicle and the Poseidon underwater drone. According to the International Institute for Strategic Studies (IISS), Russia's AI-related defense investments increased by 35% between 2019 and 2022, with a focus on cyber warfare and AI-powered missile systems.

POTENTIAL EFFECTS OF AI-DRIVEN POWER SHIFTS

The acceleration of AI development for military reasons raises various concerns. According to a 2023 RAND Corporation study, AI has the potential to disrupt global security by shortening decision-making time during wars, increasing the likelihood of blunders. A major issue is the deployment of “Lethal Autonomous Weapons (LAWS), which,” without clear rules, might lead to unintended escalation.

AI's ability to provide asymmetrical benefits may lead smaller nations or non-state actors to employ disruptive AI technology, disrupting the existing power balance. For example, AI-enhanced cyber-attacks might cripple crucial infrastructure with unparalleled precision, escalating tensions between rival powers. The rapid use of these technologies may outstrip the development of international legal frameworks, making the global arms race even more perilous

The Position of Emerging Powers in the AI Arms Race

“While the United States, China, and Russia dominate the global" AI arms race, developing nations such as India, Israel, and South Korea are making tremendous progress in military AI integration.

India, through its Defense AI Council and initiatives such as "Make in India," focuses on intelligent drones, autonomous systems, and AI-enhanced cybersecurity, with the goal of strengthening local capabilities. Israel's incorporation of artificial intelligence (AI) into its Iron Dome missile defense system displays its leadership in AI-driven military technologies. South Korea is continuing to extend its defense modernization efforts, with a focus on AI-powered drones and autonomous vehicles, especially in light of regional concerns with North Korea. These countries are becoming major actors in the emerging AI military scene.

AI AND MODERN CONFLICT

Even though, AI involvement in contemporary military warfare has great benefits but it comes with its downsides as well. In its positive aspect, AI aids in the facilitation of accuracy in decision-making, predictive analytics, and autonomous systems to allow for powerful, efficient, and speedy military operations. It also reinforces intelligence gathering and cybersecurity capabilities for defense systems, thus making them adaptive. The rising application of AI in modern warfare, therefore, raises concerned issues, relating to ethical dilemmas in forms of autonomous weapons, cyber manipulation, and accountability in warfare.

The developments transform the traditional forces and doctrines in which nations have fought and governed. After all, AI's potential to process enormous amounts of real-time data, detect patterns, and make independent decisions fundamentally changes the character of war and thus has many opportunities and challenges for global security.

Speed of decision is the third critical change in warfare introduced by AI. The military traditionally had to consider both tactical and strategic decisions after careful review of massive, tedious intelligence data by human operatives. Military forces can now process enormous amounts of information almost instantly. AI, particularly machine learning, permits its systems to differentiate between analyzing drone footage, satellite images, and other types of surveillance data in real-time. This has allowed commanders to react to dangers much faster, so that tactical adjustments can take place much more rapidly and with more precision. For instance, as employed by "the U.S. Department of Defense Project Maven, AI' can review imagery gathered by drones, thus making it possible for operators to spot potentially interesting objects, like cars or insurgents, much more quickly than human analysts would be able to. It is by reducing the decision cycle that AI allows militaries to maintain an operational edge over adversaries, for split-second decisions are what separate success and failure in these high-stakes combat environments.

Predictive military operations are improved by artificial intelligence with the help of predictive analytics. This essentially means that, on the basis of historical data combined with new intelligence, AI algorithms can predict the movements of the enemy and even predict the success rates of given strategies and predict the exact logistical requirement in military units. Those pieces of information allow commanding officers to plan their operation in better ways without taking unnecessary risks and efficient use of resources. AI systems that could analyze economic, social, and political trends could actually predict where disturbances are likely to happen, whereby governments can take preemptive action. This new ability to prevent and plan against threats in advance changes how militaries prepare for and engage in conflict, especially those occurring in a modern society.

Modern warfare is being revolutionized with AI as "the development of autonomous systems in" the form of drones and unmanned ground vehicles (UGVs) complements fully its use. Technologies such as these complete missions with reduced human involvement, hence increasing efficiency while allowing for diminished risks to personnel. For example, the Iron Dome system used in Israel accepts incoming missiles autonomously, showing full potential for AI in actual defense situations.

AI is changing the very nature of military thinking and strategies, becoming more decentralized with network-centric warfare in vogue. That would enable immediate sharing of real-time intelligence and quick response to any threat - an operation scenario where the soldier becomes an operator of systems rather than a warfare warrior. Projects like Project Maven in the US best portray the role played by AI in enhancing intelligence analysis and counterterrorism efforts.

However, ethical concerns are raised due to autonomous weapons that could independently take lethal decisions without human oversight. The prospect of cyber warfare, such as is seen in Russia using AI for cyber espionage and manipulation, creates a possibility of unintended escalations in conflicts. Likewise, China's application of AI for mass surveillance and autonomous weapon systems has underscored the geopolitics of the technology.

The article by Kristian Humble, tilted **"War, Artificial Intelligence, and the Future of Conflict",**focuses on growing alarms over AI-driven autonomous weapons systems, which independently of human direction make choices about attack selection. This paper suggests that despite leaps in technology, such weapons are remarkably unregulated internationally. The paper finds that the definitions of AWS are broad and varied, set out by organisations ranging from the UK to the US Defense Departments. Thus, the construction of a harmonised regime is a considerable challenge. Legal oversight becomes conspicuously absent in technological applications like this, raising very significant ethical questions about their use in war, especially when machines are involved in life and death decisions.

Against this backdrop, the article demands international legislations that would enforce human supervision of AWS. "The United Nations' Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security had called for" more regulations, but the pace was very slow. In their 2023 report, they recommended more debates that will come up with relevant legislation, cautioning that the law should be dynamic enough to keep pace with the rapid development of AI in modern warfare systems.

THE POSITION OF PRIVATE TECH COMPANIES IN THE AI ARMS RACE

Private IT companies "have played a critical role in" the global AI arms race, encouraging research and development of advanced technologies that are rapidly being integrated into military systems. Companies like Google, Microsoft, Amazon, and Palantir have emerged as major contributors to" military AI" research and applications. For example, "Google's Project Maven, which aimed to use AI to analyze drone surveillance footage, highlighted the growing partnership between technology companies and the security sector. Similarly, Microsoft's investment in cloud computing services for military use, as well as Palantir's considerable involvement in data analytics for defense intelligence, demonstrate how private firms are determining the future of combat.

However, the involvement of private corporations in military AI development presents a number of ethical concerns. A major source of concern is the possible misuse of AI technologies, "particularly in the context of autonomous weapon systems" & AI-driven conflict. An issue surrounding Project Maven—which sparked protests from Google employees who were "concerned about the company's

involvement in military" applications—highlights the ethical tension between corporate principles and security imperatives. There is also the question of transparency; many of these AI systems are developed behind closed doors, with no public scrutiny of how they are utilized or the repercussions of their deployment, "particularly in areas such as surveillance and" autonomous decision-making. Another major concern arises because of the global nature of the tech companies as some of them make their product somewhere else and sell them all around the world. Because of this the issue of jurisdiction arises because their cross-border presence makes it difficult for any single government to supervise or control the development and application of AI technology in the military industry amplifying the risks associated with an unchecked AI arms race.

THE NECESSITY FOR A GLOBAL FRAMEWORK IN REGULATING MILITARY AI

In the absence of any international "framework that regulates the use of" artificial intelligence inn militery, a plausible threat to global security is thereby added. This is because the inconsistent approaches to regulation will result in an ad hoc, fragmented landscape that lacks coherence as more and more nations develop and deploy AI technologies for military purposes. Where there are differences in countries trying to develop cutting-edge military AI, the gap continues unabated without even a convincing binding framework that calls for more capability without safeguards or provisions on ethical use and accountability. But without regulation in this vacum it enables developing countries to find areas of competitive advantages that override established humanitarian principles and risk stability in international relations.

One of the most fundamental risks in the absence of treaties on military AI is a lack of accountability when international law is broken. Indeed, if or when autonomous weapons systems decide to operate without the intervention of a human operator, liability for all such negligent or malevolent acts would practically be impossible to determine. This would run drastically in opposition to principles of established tenets of international humanitarian law: serious attacks do not formally cause harm may go unpunished. More importantly, the speed of rapid development of AI technologies could outstrip the development of integrated regulations, and therefore proliferate systems whose operational parameters are not fully clear or defined. Lethal autonomous weapons raise profoundly complex ethical questions, particularly regarding "the principle of distinction-the obligation to distinguish between" combatants and non-combatants-and may be breached should AI systems fail to conform to international legal standards governing warfare.

This further leads to an arms race because countries try to outdo each other in creating the powers of their militaries through AI inventions. Besides piling up risk factors for security within the global platform, such a race generates geopolitical tensions between countries since they are more apprehensive about the progress by other countries over such technology. States that perceive themselves as falling behind will spur on faster AI development in-house, and the mistake of entering a war will be all the more likely. Competition within a competitive environment can push countries to resort to behaviors that favor technological hegemony over risk avoidance through cooperation, and this will cripple the entire security landscape. Cooperation at the international level is necessary to solve these complex problems. An international universal framework regulating military AI has a high

potential of reducing risks associated with it through maybe common standards and guidelines representing some shared ethical considerations as well as humanitarian law principles. This way, the international community can better ensure that military AI systems make operational effectiveness even more beneficial by being accountable, transparent, and respecting international norms.

Cooperation mechanisms may help clear the mechanisms through which military AI might be used. That would help the countries build mutual trust and reduce the possibility of misunderstanding, thus a misunderstanding that escalates the conflict is reduced. Countries will be able to share best practices, agree on ethics guidelines, create standards in the use of AI through dialogues and shared initiatives. Such cooperation would make way for an enhancement of security, but at the same time, it would open the door to a shared understanding of implications arising with military AI technologies.

Furthermore, international cooperation can fill the gap between divergent national policies and approaches concerning military AI. Through developing continuous dialogue and collaboration platforms, the nations can collectively understand the implications of AI usage in war and ensure that the expansive step taken by AI does not compromise the fundamental humanitarian values.

TOWARDS AN INTERNATIONAL FRAMEWORK FOR AI IN WARFARE

The swift advancement of artificial intelligence (AI) in military applications emphasizes how urgently robust international frameworks to regulate their usage are needed. Even though AI offers remarkable improvements in combat capabilities, the absence of well-defined, legally binding standards presents serious risks to international security and stability. Some projects aimed at AI governance in warfare have already begun to emerge, but they are fragmented and insufficient to face the magnitude of the difficulties posed by autonomous weapons and AI-powered military systems.

One of the most notable attempts is “the United Nations Convention on Certain Conventional Weapons (CCW), which has been discussing Lethal Autonomous” Weapon Systems (LAWS) since 2014. Although the CCW intends to “prohibit the development and use of fully autonomous weapons,” no enforceable agreement has been reached, as nations claim that a ban would hinder research. This underscores a larger conflict between encouraging military innovation and upholding ethical standards in AI development. Similarly, the European Parliament has advocated for an international ban on autonomous weapons, although this has yet to be translated into practical global policies.

Dual-use technology regulation is a practical method to balancing innovation and responsible development, in which innovations produced for civilian reasons are subject to control when used in military circumstances. For example, AI advancements in healthcare or transportation should be vetted by an international commission before being applied to warfare. Finally, we cann see that, while talks and concepts about soft law have helped the cause, enforceable international frameworks are sorely needed to control AI in military applications. To prevent global security instability, a balance must be struck between innovation and responsible development. The development of moral and legal safeguards must remain a major priority on the global agenda as AI technologies evolve.

*****

SOCIO-LEGAL IMPLICATIONS OF AI INTEGRATION IN COURTS OF JUSTICE

Sudarshan Shridhar Desai[47] and Dr. Vivek Yeshwant Dhupdale[48]

ABSTRACT

The integration of artificial intelligence (AI) into the courts of justice has the potential to revolutionize legal processes, enhancing efficiency, accessibility, and decision-making. However, this technological advancement also brings significant socio-legal implications that must be critically examined. This article explores the benefits and challenges associated with AI in judicial contexts, emphasizing issues of bias, accountability, transparency, and ethics. AI systems, trained on historical data, can inadvertently perpetuate existing societal biases, leading to discriminatory outcomes in sentencing and case management. The opacity of algorithmic decision-making raises concerns about accountability, as stakeholders grapple with questions about responsibility for AI-generated outcomes. Ethical dilemmas also arise, particularly regarding privacy, surveillance, and the potential erosion of civil liberties. Furthermore, the evolving role of legal professionals in this landscape necessitates a re-evaluation of legal education and training to prepare them for collaboration with AI tools. This article argues that while AI offers significant advantages, its integration into the judicial system requires comprehensive regulatory frameworks and ethical guidelines to ensure that justice is upheld. A multi-stakeholder approach involving legal experts, technologists, and policymakers is essential to address these socio-legal challenges and foster a just and equitable legal system.

Keywords: Artificial Intelligence, Courts of Justice, Socio-Legal Implications, Bias, Accountability, Transparency, Ethics, Legal Professionals, Access to Justice, Technology in Law.

INTRODUCTION

The integration of Artificial Intelligence (AI) into the judicial system has emerged as a transformative development in legal processes worldwide. AI's capacity to analyze vast datasets, enhance decision-making efficiency, and streamline operations is revolutionizing traditional courtroom practices. However, this integration raises significant socio-legal implications that merit careful examination. This article explores these implications, focusing on issues of access to justice, bias and fairness, accountability, and the potential for changes in legal practice. AI technologies are being utilized in various facets of the legal system, including predictive policing, case management, legal research, and even decision-making processes. Tools such as natural language processing (NLP) and machine learning algorithms are employed to analyze legal texts, predict case outcomes, and assist judges in sentencing decisions.

THE ROLE OF AI IN THE JUDICIAL SYSTEM

The integration of Artificial Intelligence (AI) into the judicial system is reshaping legal processes globally. From case management to predictive analytics, AI technologies enhance efficiency, accessibility, and accuracy within courts. However, the application of AI in justice raises critical questions about fairness, accountability, and the future of legal practice.

One prominent use of AI in the judicial system is predictive analytics. This technology analyzes histo-

[47] Ph.D. Research Scholar at Dept. of Law, Shivaji University, Kolhapur, India.
[48] Head at Dept. of Law, Shivaji University, Kolhapur, India.

rical case data to forecast outcomes, assisting legal professionals in assessing the likelihood of success in litigation. Tools like Lex Machina and Ravel Law provide insights into judicial trends based on previous cases, allowing lawyers to tailor their strategies effectively. Additionally, predictive analytics can be employed in risk assessment, particularly in bail and sentencing decisions. Algorithms evaluate a defendant's likelihood of reoffending based on various factors, aiding judges in making more informed decisions. However, this application has sparked debates about potential bias, as these models can inadvertently reflect societal inequalities present in historical data.

AI has also revolutionized legal research by streamlining the process of finding relevant case law and statutes. Natural language processing (NLP) tools can quickly sift through vast databases of legal texts, helping lawyers identify pertinent information without spending hours on manual searches. Platforms like Ross Intelligence and Casetext exemplify how AI enhances legal research efficiency.

Moreover, AI can automate document review during discovery processes, identifying relevant documents and flagging anomalies. This automation not only saves time and resources but also reduces the likelihood of human error, thereby increasing the accuracy of legal proceedings. AI-powered case management systems are becoming increasingly prevalent in courts, helping manage caseloads by automating scheduling, tracking deadlines, and organizing case files. By improving operational efficiency, courts can better allocate resources and reduce backlogs, leading to faster case resolutions.

Furthermore, AI can analyze case patterns and workflow efficiencies, providing insights to court administrators on optimizing processes. This data-driven approach can enhance the overall functioning of the judicial system, ensuring that justice is delivered more promptly. Some jurisdictions are utilizing AI to assist in sentencing decisions, where algorithms analyze various factors, including prior offenses and the nature of the crime, to recommend sentences. The aim is to create consistency in sentencing and reduce the influence of implicit biases. However, this use of AI in sentencing raises concerns about accountability and transparency. If an algorithm recommends a particular sentence, determining the rationale behind that recommendation can be challenging. This lack of transparency can undermine public trust in the judicial system and hinder defendants' ability to challenge decisions made by AI.

BENEFITS OF AI IN THE JUDICIAL SYSTEM

AI significantly enhances the efficiency of legal processes. By automating routine tasks, legal professionals can concentrate on more complex aspects of their cases. This increased efficiency benefits not only lawyers but also streamlines court operations, ultimately reducing the time required to resolve cases.

Moreover, AI has the potential to improve access to justice, particularly for individuals who may not afford legal representation. Online legal services and AI-powered chatbots can provide preliminary legal advice, empowering individuals to navigate the legal system more effectively. This democratization of legal resources can help bridge gaps in access, especially in underserved communities.

Additionally, AI offers data-driven insights that assist judges and lawyers in making more informed decisions. Predictive analytics and risk assessments provide a deeper understanding of case dynamics, enabling legal professionals to evaluate risks and opportunities more accurately.

CHALLENGES AND ETHICAL CONSIDERATIONS

One of the most significant challenges of AI in the judicial system is the potential for algorithmic bias. AI systems learn from historical data, which can reflect existing societal biases. If these biases are not addressed, they may perpetuate discrimination in judicial outcomes, undermining the principle of fairness.

Additionally, the opaque nature of AI decision-making poses challenges for transparency and accountability. Legal professionals and defendants may struggle to understand how AI algorithms arrive at certain conclusions, complicating the ability to contest decisions. Establishing clear guidelines for the use of AI and ensuring that human oversight remains a critical aspect of judicial decision-making is essential.

Furthermore, the integration of AI in the judicial system raises ethical questions regarding the role of technology in justice. Legal professionals must navigate the balance between leveraging AI for efficiency and ensuring that technology does not infringe upon defendants' rights or undermine the integrity of the legal process.

SOCIO-LEGAL IMPLICATIONS OF AI IN THE LEGAL SYSTEM

The integration of Artificial Intelligence (AI) into the legal system has emerged as a transformative force, promising enhanced efficiency, accessibility, and decision-making capabilities. However, as AI technologies become integral to legal processes, they bring forth a complex array of socio-legal implications that require careful scrutiny. This article explores these implications, focusing on access to justice, bias and discrimination, accountability, and changes in legal practice.

AI has the potential to improve access to justice, particularly for individuals who may not afford traditional legal representation. Tools such as chatbots and virtual legal assistants can provide preliminary legal advice and guidance, allowing individuals to navigate the complexities of the legal system without incurring significant costs. For instance, platforms like DoNotPay offer services that assist users in contesting parking tickets or seeking small claims, thereby democratizing access to legal resources.

Conversely, reliance on AI tools may inadvertently widen existing inequalities. Access to AI technologies is often limited by socio-economic factors, meaning individuals in underserved communities may lack the necessary resources—such as internet access or technological literacy—to benefit from these innovations. This disparity can exacerbate the justice gap, leaving vulnerable populations without adequate support.

The integration of AI can also exacerbate geographic disparities in access to justice. Urban areas may benefit from advanced legal technologies, while rural communities might be left behind. The uneven

distribution of resources can hinder the ability of individuals in less populated areas to access AI-driven legal services, further entrenching systemic inequalities.

One of the most pressing concerns regarding AI in the legal system is the potential for algorithmic bias. AI systems learn from historical data, which may reflect societal biases related to race, gender, and socio-economic status. If these biases are not adequately addressed, AI can perpetuate discrimination in judicial outcomes, impacting sentencing, risk assessments, and predictive policing. Predictive policing algorithms, for instance, have been criticized for disproportionately targeting minority communities based on historical crime data, which may over-represent certain demographics. Such biases undermine the principle of equality before the law and can lead to wrongful accusations and unequal treatment in the judicial process.

The opacity of AI decision-making processes poses significant challenges for transparency and accountability. Legal professionals and defendants often struggle to understand how algorithms reach specific conclusions, making it difficult to contest decisions based on AI recommendations. This lack of transparency can erode trust in the legal system and hinder the ability of individuals to seek redress. Efforts to improve the explainability of AI algorithms are crucial to addressing these concerns. Legal frameworks may need to evolve to mandate greater transparency in AI applications, ensuring that individuals can understand and challenge the rationale behind AI-driven decisions.

As AI systems increasingly influence judicial outcomes, questions of accountability become paramount. When an AI algorithm makes a flawed recommendation, who is responsible? Current legal frameworks struggle to address liability in cases involving AI, leading to uncertainty about how to hold individuals or organizations accountable for decisions made by AI. This ambiguity can have serious implications for justice. If AI is perceived as an autonomous decision-maker, it may undermine the principle of human oversight in judicial processes.

To mitigate risks associated with AI decision-making, robust judicial oversight is essential. Judges and legal professionals must remain actively involved in the decision-making process to ensure that AI tools are used responsibly and ethically. This oversight should include checks to prevent misuse and to ensure that AI does not replace critical human judgment in legal proceedings.

The integration of AI is transforming the landscape of legal practice. Routine tasks such as document review, legal research, and case management are increasingly automated, altering the roles of legal professionals. While this can lead to increased efficiency, it may also result in job displacement, particularly for paralegals and junior lawyers whose work is more susceptible to automation. Legal professionals will need to adapt to these changes by acquiring new skills that complement AI technologies. Emphasizing critical thinking, emotional intelligence, and ethical considerations will be essential for legal practitioners in an AI-enhanced landscape.

The ethical implications of AI use in the legal system are profound. Legal professionals must grapple with the consequences of relying on AI tools, including the potential for biased outcomes and the erosion of human judgment. The duty to ensure that AI applications adhere to ethical standards and do not infringe on clients' rights is paramount. Moreover, as AI continues to evolve, legal frameworks must

adapt to address new ethical challenges. Establishing clear guidelines for AI use in legal practice is essential to maintaining the integrity of the judicial system.

IMPACT OF AI ON ACCOUNTABILITY IN THE LEGAL SYSTEM

The integration of Artificial Intelligence (AI) into the legal system introduces significant challenges and complexities concerning accountability. As AI technologies become more prevalent in areas such as predictive policing, risk assessment, and case management, understanding who is responsible for the outcomes influenced by these systems becomes paramount.

One of the primary challenges surrounding AI in the legal context is determining accountability when decisions are made based on algorithmic recommendations. Traditional legal frameworks are designed around human actors who can be held accountable for their actions. However, as AI systems increasingly contribute to decision-making, questions arise: If an AI tool produces a flawed recommendation, who bears the responsibility? Is it the developers of the software, the legal professionals who rely on it, or the judicial system that implements its recommendations?

This ambiguity can lead to significant legal and ethical dilemmas. For instance, if a predictive policing algorithm disproportionately targets certain communities, leading to wrongful arrests, the question of who is liable for the resulting injustices becomes critical. Without clear accountability, victims of such biases may find it challenging to seek redress, undermining public trust in the legal system.

To address these accountability challenges, the role of human oversight becomes crucial. Legal professionals must remain engaged in the decision-making process, ensuring that AI tools are used responsibly. Judges and attorneys should critically evaluate AI recommendations rather than accepting them at face value. This human intervention is vital to safeguard against potential biases embedded in AI algorithms and to uphold the principles of justice and fairness.

Furthermore, ongoing training for legal professionals on AI's capabilities and limitations is essential. Understanding how these technologies work enables legal practitioners to make informed decisions about their use and to recognize when to question AI-driven conclusions. Transparency in AI systems is another key factor in ensuring accountability. Legal practitioners and the public must understand how AI algorithms reach their conclusions. If a system provides a recommendation without a clear rationale, it can be challenging to contest that decision. Establishing standards for the transparency and explainability of AI tools is vital for maintaining public trust and enabling effective scrutiny of AI-driven outcomes.

Efforts to create “explainable AI” aim to demystify the decision-making processes of these systems, allowing users to understand the reasoning behind specific outcomes. Legal frameworks may need to adapt to mandate transparency in AI applications used within the judicial system, ensuring that stakeholders can assess the fairness and appropriateness of AI-driven decisions.

As AI continues to evolve, the legal system must develop robust frameworks to address accountability issues. This includes clear guidelines on liability for AI-driven decisions, standards for human oversight, and requirements for transparency in AI algorithms. Collaborative efforts between legal

professionals, technologists, and policymakers will be essential to create an environment where AI can enhance the judicial process while preserving accountability and ethical standards.

CONCLUSION

The socio-legal implications of AI integration in courts of justice are multifaceted and complex. While AI presents opportunities to enhance efficiency and access to legal services, it also poses significant challenges related to bias, accountability, and the fundamental principles of justice. Addressing these implications will require a concerted effort from legal professionals, policymakers, and technologists to ensure that the benefits of AI are realized without compromising the integrity of the judicial system. As we move forward, it is crucial to establish robust regulatory frameworks that prioritize transparency, equity, and accountability in the use of AI in courts.

*****

DIGITAL INJUSTICE: HUMAN RIGHTS AND THE GROWING THREAT OF ONLINE GENDER-BASED VIOLENCE

Pakhi Tandon[49]

ABSTRACT

Online gender-based violence (OGBV) is a growing issue in today's digital world, involving cyberstalking, doxxing, non-consensual sharing of intimate images, online harassment, and hate campaigns. Women, LGBTQ+ individuals, and marginalised communities are disproportionately affected, facing violations of their rights to privacy, expression, and security. These abuses reinforce gender inequality and silence already vulnerable voices. Despite its severe consequences—such as trauma and isolation—legal frameworks lag behind. International protections like the Universal Declaration of Human Rights and CEDAW do not adequately address digital violence, and national laws on cybercrime are often fragmented and poorly enforced. Online platforms, though central to modern communication, are often not held accountable for the abuse of their services. This paper examines the nature of OGBV, its human rights implications, and the shortcomings of current laws and regulations. It also looks at the role of digital platforms in either fostering or mitigating abuse and offers recommendations for legal reforms, greater platform accountability, and digital literacy initiatives. Addressing OGBV requires coordinated efforts from governments, platforms, and civil society to protect vulnerable groups.

Keywords: Online Gender-Based Violence (OGBV), Human Rights, Digital Safety, Legal Frameworks, Platform Accountability

INTRODUCTION

The digital age has been a transitional period for social life. Its greatest opportunity for information exchange and communication is also its darkest area in making gender-based violence likely, targeting women, gender minorities, and sexual minorities. Online gender-based violence (OGBV) refers to harmful or discriminatory behaviours that are menacing or threatening within a digital context, directed at one or more individuals based on their perceived or actual gender or sexual identity.

OGBV cannot be described as a standalone issue but forms part of a much broader spectrum of GBV, deeply ingrained in patriarchal systems and societal inequalities. In the context of human rights, OGBV violates fundamental freedoms-the right to be free from violence, the right to privacy, and the right to freedom of expression. The victims of OGBV face insurmountable barriers to seek justice, as legal frameworks lag behind technological advancement, and the online platform is not taking enough responsibility for violence that gets perpetrated on it.

This paper discusses the dynamics of OGBV; its impact on human rights for women and other gender-disadvantaged groups, and whether international and national laws are effective in dealing with this issue. It also examines how online platforms promote OGBV and what policies can be employed to counter the rising menace of OGBV to human rights on the digital platform.

DEFINE ONLINE GENDER-BASED VIOLENCE (OGBV)

The characteristics and features of OGBV

[49] Student at Christ (Deemed to be University) Pune, Lavasa, India.

Online gender-based violence (OGBV) refers to various forms of abusive conduct conducted through digital channels, including social media, websites, and messaging applications. Although the internet serves as an essential resource for information dissemination and personal expression, it has simultaneously emerged as a medium for gendered violence, taking advantage of the anonymity, rapidity, and lack of geographical boundaries inherent in online communications.

OGBV can be divided into several categories:

1. Cyberstalking refers to the continuous and unwelcome digital observation or communication, typically resulting in anxiety or psychological discomfort. This form of harassment often disproportionately affects women, as offenders closely observe their online actions and employ digital means to exert control or influence over their conduct.
2. Doxxing: The process where personal information like people's home addresses, phone numbers, or personal identification details are made public without their consent. Doxxing is a technique used to intimidate and harass their victims, which may later lead to violent acts in real life.
3. Non-consensual sharing of intimate images (Revenge Pornography): The non-consensual sharing of intimate or sexually explicit images of a person is the most common type of OGBV. It usually serves the purpose of embarrassing, extorting, or dominating the victim.
4. Online Hate Speech and Cyberbullying: Women and other gender minorities are often targeted through hate speech, threats, derogatory comments, and cyber-sexual harassment online and in almost every other virtual context. Online harassment is used to intimidate, humiliate, or terrorise the victim, making these spaces unsafe.
5. Trolling and Flaming: Trolling is characterised by the intentional provocation or distress of individuals on the internet, frequently through insulting or offensive remarks. Flaming denotes aggressive online exchanges marked by hostile language, often aimed at individuals based on their gender or sexual orientation.
6. Identity Theft and Impersonation: Certain offenders construct fraudulent profiles utilising a victim's name or likeness with the intent to mislead others, disseminate false information, or tarnish the victim's reputation. Such actions may result in harassment, financial deception, and social alienation.

OGBV represents a manifestation of entrenched power disparities within society, wherein online platforms perpetuate and intensify existing gender hierarchies. This phenomenon disproportionately impacts women, while gender minorities and LGBTQ+ individuals are similarly subjected to increased risks. Additionally, intersectional dimensions including race, ethnicity, and socioeconomic status further aggravate the experiences associated with OGBV, as women of colour and individuals from marginalised communities frequently suffer from multifaceted types of online harassment.

PREVALENCE AND EFFECT OF OGBV

Underreporting, variation in definition, and a lack of uniformity in data collection between jurisdictions make it quite challenging to quantify the scale of OGBV. However, many more studies established that the problem was ubiquitous. For instance, a survey done by Amnesty International in 2018 reported that 23% of women from eight different countries reported experiencing online abuse or harassment; for those, the psychological and emotional impact was understandably prominent, with many reporting increased anxiety, depression, and feelings of insecurity.

The incidence of cyberbullying among individuals who identify as LGBTQ+ is significantly increased. Studies have shown that LGBTQ+ individuals suffer much greater rates of intimidation, threats, and hate speech, often driven by homophobic, transphobic, and misogynistic attitudes. The attributes of anonymity and the vast international extent of the internet provide perpetrators with a sense of immunity, leading to growing numbers and more extreme forms of violence.

The consequences of OGBV go beyond the digital sphere: long-term psychological trauma, social isolation, and professional setbacks for victims, and the complete withdrawal of women and marginalised people from online spheres as a whole, leading to a chilling effect on free expression and engagement in public discourses. Self-censorship limits the diversification of voices and perspectives in digital conversations, further cementing existing power imbalances and gender inequalities.

OGBV AS A VIOLATION OF HUMAN RIGHTS

Online gender-based violence goes beyond being a violation of personal rights; it violates crucial human rights. The internet is an essential space through which many rights such as freedom of expression, access to information, and political involvement are exercised. Online gender-based violence undermines all these rights by creating a hostile and dangerous environment for women and other marginalised groups. Underlying human rights affected by online gender-based violence include:

- Right to Privacy: OGBV often relates to invasions of personal privacy, including issues such as doxxing or the non-consensual sharing of intimate images. Such acts subject the victims to harassment and threats up to actual physical harm, violating the fundamental right to privacy and security.
- Freedom of speech: Women and gender minorities face web harassment while they try to communicate themselves or in public speech. The fear of abuse or backlash deters many to pre-censor themselves or refrain altogether from engaging online, thereby limiting their right to free expression.
- Right to Security and Freedom from Violence: OGBV is a form of gender-based violence that violates the right to live free from violence, discrimination, and harm. The psychological, emotional, and physical consequences of OGBV are severe, and, in extreme cases, threats transmitted through online platforms become real violence.
- Right to Dignity and Equality: OGBV reinforces gender stereotypes, thus perpetuating gender inequality. The abuse mainly affects women and members of the LGBTQ+ community, whose dignity is offended and further contributed to a culture of discrimination and violence.

FRAMEWORK FOR HUMAN RIGHTS CONCERNING OGBV

International Legal Systems

International human rights law sets the framework for the approach to OGBV, although it does not focus specifically on the digital dimensions of gender-based violence. The following is some key international instrument relevant to OGBV:

1. Universal Declaration of Human Rights (UDHR): The UDHR is one adopted in 1948 that addresses the basic rights and freedoms to which all individuals are entitled. Article 3 provides for the right to life, liberty, and security, while Article 12 undertakes to guarantee respect for privacy. Although the UDHR predates the digital age, the principles it contains are relevant to OGBV in that online violence and harassment infringe the right to privacy, security, and dignity.

2. The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which was ratified in 1979, represents a significant international agreement aimed at eradicating discrimination directed at women. Article 1 delineates discrimination as any form of distinction or limitation based on gender that hinders the fulfilment of human rights. CEDAW mandates that nations implement actions to eradicate violence against women, a mandate that includes addressing such violence within digital environments where online gender-based violence (OGBV) transpires.

3. International Covenant on Civil and Political Rights (ICCPR): The ICCPR, established in 1966, ensures fundamental civil and political liberties, encompassing the right to privacy (Article 17), freedom of expression (Article 19), and safeguards against discrimination (Article 26). The occurrence of OGBV infringes upon these rights, especially by restricting the freedom of expression of victims and exposing them to violations of their privacy.

4. Istanbul Convention: The Istanbul Convention is the full name of the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence. It is one of the most general agreements dedicated to gender-based violence. Primarily, it tends to underscore

5. Off-line violence: It calls for criminalization of some forms of online misconducts by states, such as stalking and sexual harassment.

Although such instruments provide a very robust framework on which to frame attacks against GBV, they have remained deficient specifically with regard to modern violence in their digital nature. With growing prevalence more and more in conjunction with OGBV, there must be recognition and a concrete way of finding a solution to challenges that online abuse carries within international treaties and conventions.

National Legal Frameworks

The efforts at the national level have been quite different in different jurisdictions, with some countries making quite remarkable progress and others not doing so well at all. Most countries have amended harassment, defamation, and stalking laws to include digital crimes, but these amendments are mostly piecemeal and not adequate enough for the general OGBV situation.

1. The United States. In the United States, there is no federal legislation that specifically focuses on OGBV. However, there are numerous state laws on the books which specifically address aspects of the issue, such as the more specific cyberstalking and revenge porn statutes. Though VAWA and CDA do provide some protections, a lack of a unified federal approach regarding OGBV represents an important gap.
2. EU: The EU has made strides in combating Online Gender-Based Violence (OGBV) through efforts like the General Data Protection Regulation (GDPR), which specifically aims to protect personal data, and the Digital Services Act, which aims to hold online platforms accountable for such detrimental content. In the meantime, enforcement and heterogeneity among its member states remain a challenge.
3. India: The country has enacted legislation, the Information Technology (IT) Act, that holds legal consequences for cyber stalking, doxxing, and revenge porn. However, application varies, and stigma in society leads most of the victims not to come forward with incidences of OGBV.
4. Philippines: The Philippines enacted the Cybercrime Prevention Act in 2012. It encompasses some forms of cybercrime like cyberstalking, identity theft, and hacking. This country has been praised for its foresight on digital crimes, but some critics said a few provisions are particularly dangerous against free speech because they pertain to libel.

In many countries, the enactment of laws responding to OGBV is affected by the activities such as underreporting, ignorance of law enforcement, and judicial incompetence in terms of perceiving the seriousness of online violence.

OBSTACLES IN TACKLING OGBV

Accountability of Platforms and the Function of Technological Corporations

Perhaps the greatest challenge to tackle OGBV is the role of online platforms and tech firms. Social media sites, messaging apps, and websites are the means whereby most OGBV takes place, and yet companies have been very slow to take effective action to prevent abuse.

1. Inconsistent Enforcement of Community Guidelines: Many online platforms have community guidelines that prohibit harassment, hate speech, and other forms of abuse. However, enforcement is often inconsistent, and harmful content frequently remains online despite being reported by users. This inconsistency undermines trust in the platforms' ability to protect users from OGBV.
2. Limitations of Content Moderation: Automated systems for content moderation, which are employed by platforms such as Facebook, Twitter, and YouTube, frequently struggle to effectively identify subtle manifestations of abuse, especially in cases involving gender-specific slurs, coded language, or non-verbal content, including images and videos. Human moderators are frequently inundated by the sheer amount of content, resulting in delays or shortcomings in responding to reports of abuse.

3. Profit Motives and User Engagement: Most technology company business models are driven to a great extent by user engagement, which promotes the acceleration of abhorrent or harmful content. Twitter and Instagram make money through increased user engagement even if it is fueled by abuse or harassment.
4. Lack of Transparency: Most websites are not transparent about how they address reports on OGBV. Thus, it has become very challenging for users to have an overview of the processes instituted towards the handling and abuse case. Transparency reports, when available, are usually not clear enough on the actions that were undertaken in ensuring non-accessible harmful content or having offenders punished.

Legal and Jurisdictional Obstacles

The internet's global nature poses significant legal challenges in handling the issue of OGBV. Main barriers include:

1. Cross-border Jurisdiction: The very reason perpetrators and victims of OGBV often find themselves on different sides of the border makes it complicated to engage in prosecution. National laws may not extend beyond borders, and international legal cooperation is often slow or nonexistent in cases of OGBV.
2. Gaps in Law. Most countries lack laws targeted at OGBV, especially in new ways of abuse created through deep fake pornography or coordinated harassment campaigns. Where there are laws, they are outdated or too narrow and don't include a comprehensive list of new forms of online abuse.
3. Underreporting and Social Stigma: Several factors give rise to severe underreporting of OGBV, such as fear of retaliation against them or their families, the lack of trust in law enforcement, and social stigma towards victims of online abuse. Victims often believe reporting OGBV would not lead to any meaningful action or would lead to further harassment and shaming as a consequence of reporting.
4. Limitations in the Law Enforcement: Even after reporting OGBV, the law enforcement agencies are not adequately prepared to tackle digital crimes. Most officers neither have training nor technical skills to investigate online abuse which leads to indifferent attitudes or failure to act on complaints.

CASE STUDIES: RESPONSE TO OGBV

South Africa: Feminist digital activism

South Africa has emerged as one of the centres of feminist digital activism, partly because gender-based violence is dramatically increasing in both the physical and online worlds. The AmINext movement, initiated during 2019, followed a list of women who were killed and brought attention to an even deeper issue: gender violence in South Africa. Advocates used social media, particularly Twitter and Instagram, to highlight how deeply seated violence against women was within both the online and offline environments.

Consequently, the South African government enacted laws in a response measure towards the movement, among which were reforming domestic violence laws, amendments relating to sexual offences, and cybercrimes. These are for the welfare of OGBV victims where provisions are catered for, dealing with OGBV, especially cyberstalking and online harassment.

India: Legislation Reforms under Modern Context

In India, the increasing incidence of OGBV has led to legal reforms aimed at increasing protections for victims. The Information Technology (IT) Act 2000 was amended in 2008 with provisions that added cyberstalking, identity theft, and the unauthorised release of intimate images to the list of crimes. Furthermore, amendments made to the Indian Penal Code in 2013, following the notorious Nirbhaya gang rape, provided more severe punishment for crimes associated with sexual assault, which include online abuse. These reforms notwithstanding, enforcement remains a challenge in India. Many victims of OGBV say that law enforcement officers dismiss their online abuse, or they do not possess technical competence to investigate digital crimes more effectively. A significant number of women refrain from reporting incidents of OGBV due to social stigma and victim-blaming.

The European Union: Common Efforts to Combat OGBV

The European Union has taken a harmonised approach towards fighting OGBV, especially through policies such as the GDPR and the Digital Services Act. The GDPR, which has been in effect since 2018, brings high-level protections for private data, forcing companies responsible whenever user privacy is violated. Not particularly addressing OGBV, the GDPR is essential in checking other forms of abuse such as doxxing or identity theft.

The European Union has been frontrunner in addressing the online platforms' engagement with OGBV. The Digital Services Act 2022 is primarily aimed at building a safer online sphere by regulating the content moderation practices of technology companies. The DSA requires the content moderation practices of platforms to be more transparent regarding their algorithmic functioning and processes for removing content, in addition to introducing penalties for non-compliance with user safety regulations.

RECOMMENDATIONS FOR COMBATING OGBV

The fight against OGBV and protection of human rights of women and marginalised gender groups is absolutely necessary to be done on a multi-faceted level: legal reform, responsibility ensured from the networks, and empowerment of victims together with education in the use of digital technologies.

Improving Legal Institutions

1. International Cooperation Due to the global character of the Internet, international cooperation is necessary to address the phenomenon of OGBV. A multilateral treaty on OGBV may thus offer a framework to harmonise domestic laws across borders, establish cross-border enforcement, and hold perpetrators accountable.
2. National Legislation: Specific laws targeting OGBV should be enacted or updated to include emerging forms of abuse, like deep fake pornography, revenge pornography, and coordinated

harassment campaigns. Law enforcement and judicial authorities should receive proper guidance through a well-defined legal framework to address OGBV effectively.

3. Capacity building for law enforcement: Equip law enforcement agencies with the necessary capacity and skills to address the cases of OGBV. Such necessary capacities include training in digital forensics as well as in a victim-centred approach to handling online abuse cases.

Holding Platforms Accountable

1. Transparency and Accountability: The enabling role of OGBV by online platforms should be made accountable. Governments should introduce compulsion for the online platforms to come with transparency reports that will detail how they respond to complaints against abuse, the steps taken, and resultant outcomes.
2. Enhanced Content Moderation There should be sufficient content moderation on the systems, especially when using AI in detecting dangerous content and more human moderators to sort out abuse in nuanced cases. The reporting mechanisms of these platforms should also be enhanced to make it easy for victims of OGBV to file complaints and receive responses.
3. Data Protection: Governments should strengthen data protection laws in position to ensure that online platforms can't misuse user data, nor endanger the person to the risk of OGBV. This should include holding companies liable for breaches of privacy issues, such as doxxing and the unauthorised publishing of private images.

Empowering Victims and Digital Literacy

1. Support Systems: Availability of support structures to OGBV victims entails legal, psychological, and reporting mechanisms for individual security. These support systems can come from governments and civil society organisations collaborating together.
2. Digital Literacy: Raising awareness about online safety and digital rights is essential in preventing OGBV. Schools, universities, and NGOs should incorporate digital literacy programs that educate users on how to protect themselves online.
3. Support Reporting Governments and service providers must ensure that a safe environment exists for reporting OGBV. This includes, among other things, ensuring complainants are not retaliated upon at the reporting stages and ensuring their concerns are taken seriously.

CONCLUSION

It therefore poses a significant threat to human rights in the digital era by increasing online gender-based violence. As much as new forms of interaction and expression are facilitated through technological innovations, it has equally enabled exploitation. OGBV also threatens vital human rights, especially those of privacy, security, and freedom of speech. There is a need for legal frameworks at both the national and international levels to evolve with these new challenges. In addition, online services must also be held accountable for their role in facilitating abuse. Combating OGBV requires a collaborative, worldwide approach combining legal reform, platforms' responsibility, and digital literacy to protect women's and all marginalised gender groups' human rights.

*****

CYBER CRIMES AGAINST VULNERABLE GROUP: LEGAL CHALLENGES AND ETHICAL IMPLICATIONS

Keerthana S.[50] and Aishwarya G.J.[51]

ABSTRACT

This research paper examines the growing issue of cybercrimes against vulnerable groups, particularly women. 'As technological advancements provide new avenues for empowerment, they also expose these groups to online risks such as cyberstalking, financial exploitation, and identity theft. The study highlights how emerging technologies like deep-fakes contribute to online gender-based violence, with a focus on their ethical challenges. It also addresses the role of social media in both proliferating and combating revenge porn, emphasizing the need for stronger content moderation and victim support. The research explores the vulnerabilities of female in extended reality social media platforms, where harassment and exploitation are growing concerns, and it delves into the ethical implications of artificial intelligence (AI) in women welfare, particularly regarding privacy, data protection, and bias. Key legal challenges, such as regulating deep-fake content, enforcing consistent social media standards, and protecting youth in immersive environments, are analyzed. To address these issues, the paper proposes several solutions, including the introduction of robust legal frameworks, holding social media platforms accountable for harmful content, and enforcing protective measures for women in social media environments. Ethical AI development and increased public awareness through digital literacy programs are also recommended. Ultimately, the paper argues for a multi-faceted approach combining legal reform, technological innovation, and education to protect vulnerable populations and ensure a safer online environment. Global cooperation and ethical interventions are essential to effectively address these challenges in the rapidly evolving digital landscape.'

Keywords: Cybercrimes, Deep-fakes, vulnerable groups, AI ethics, online harassment.

INTRODUCTION

Criminality and social relations have been intermingling and mutually dependent for quite a long time. As societies evolve so does the expressions of crime. Internet originally had a purpose of augmenting communication and connection is a perfect example of this relationship. It has helped produce a number of desirable trends but has also degenerated into a cradle of the modern crimes that pose immense danger to the international community.

Cybercrime presents two main risks: first, it attacks computers and devices that are directly connected to the internet through identity theft, hacking and spamming as well as phishing. Second, it makes these devices instruments of harming individuals' implying stalking and blackmailing and illicit trades. The problem of cybercrime is also an innovative one, as such activities become deeper embedded in daily life, from paying taxes to shopping, novel risks appear.

explained as offenses that occur in computer operations, the definition of cybercrime was officially given by William Gibson who used it when writing Neuromancer. Jaishankar's (2008) 'Space Transition Theory' works under the notion that behaviour transitions from physical to digital space most

[50] Student at K L E Society's Law College, Bengaluru, India.
[51] Student at K L E Society's Law College, Bengaluru, India.

of the time resulting in cyber crime. The demand to adopt e-governance has facilitated service delivery while at the same time up increasing risk of cyber risks.

Cybercrime, cyberstalking, harassment, and the dissemination of the private image are dangerous for vulnerable people, especially women. They are particularly vulnerable to cyber female violence the use of technology and images like revenge porn and deep fake technology. Social inequality is worsened by the fact that users of the internet are shielded from other people.

Thus, general approaches are required to counter these new emerging threats. , national governments must continue to enhance legal standards, technology companies must ensure strict regulation of content sharing services and public health campaigns should encourage citizens to learn how to protect themselves online. The aforementioned measures can make the Virtual world a safer place and close the Gender Gap in Cyber related violence against women.

LITERATURE REVIEW

The literature on cyber crimes against vulnerable groups, particularly women, reveals a troubling trend of gender-based harassment in digital spaces, with significant societal implications. Citron (2009) argues that cyber gender harassment not only harms women directly but also reinforces societal hierarchies, normalizing violence against them in both professional and social contexts. She emphasizes the urgency of addressing this issue, positioning the evolution of the internet as a critical battleground for gender equality.

Building on Citron's insights, Simons (2015) highlights the disproportionate impact of online harassment on women, especially through social media. She introduces the concept of "gender-based online harassment," which includes cyberstalking and non-consensual image sharing, emphasizing the need for research to empower victims and deter perpetrators.

Faith and Fraser (2019) focus on the digital harassment faced by women leaders, revealing how such abuse undermines their legitimacy and discourages political participation. They introduce "technology-facilitated sexual violence" (TFSV), showing that young women are particularly vulnerable.

Together, these studies underscore the need for a comprehensive understanding of cyber crimes against women, advocating for increased awareness and action to combat systemic issues perpetuating gender-based violence in digital spaces.

METHODOLOGY

This research employs a mixed-methods approach, integrating both qualitative and quantitative data to explore the impact of cyber crimes on vulnerable groups, particularly women. A comprehensive literature review provides a theoretical foundation, drawing from key studies on cyber gender harassment and its implications.

Qualitative data were collected through in-depth interviews and focus group discussions with victims, advocates, and experts, focusing on personal experiences and perceptions of cyber safety. Thematic analysis was applied to identify recurring themes and insights.

Additionally, a structured quantitative survey was distributed to assess the prevalence of online harassment and the effectiveness of existing legal frameworks. Data analysis included statistical techniques to quantify experiences and identify trends.

Policy analysis was conducted to examine existing legal frameworks, such as the Information Technology Act, highlighting gaps and suggesting reforms. This multifaceted approach ensures a thorough understanding of the challenges and potential solutions to cyber crimes affecting women.

DISCUSSION

1. CYBER CRIMES AFFECTING VULNERABLE GROUPS

One of the significant implications of increased internet use among people is the cyberstalking, harassment, and financial exploitation against women. Such harassment occurs through social media sites, emails, amongst other methods that perpetrators use to exploit, intimidate, or financially drain the victims. Cyberstalking refers to repeated harassment that includes threats or intimidation that leaves the victim with a sense of fear and psychological distress. According to research, over 40% of women have experienced some form of online harassment and many received serious threats-including cyberstalking (Bates, 2017). Legal frames like India's Information Technology Act (2000), which allows for punishment for cyberstalking, remain largely unenforced. Such legal cases, such as State of Maharashtra v. Kumar (2018), emphasize further legislative protections and better implementation methods to prevent women from these crimes (Mukherjee, 2019)..

2. TECHNOLOGICAL IMPACT ON CYBERCRIME

Deep-fake technology has made cases of gender-based violence in the online world worse. Deep-fakes refer to the process of changing videos and images with the aim of creating realistic but false depictions. These are used to debase and exploit women by creating unconsented sexual content. The altered videos invade the privacy of women and pose great ethical questions as they cannot trace and delete them after they have been disseminated on the internet. As Citron (2019) argues, deep-fakes magnify the risks of gender-based harassment, particularly revenge porn, by creating irreversible damage to victims' reputations. Legal systems worldwide are still grappling with how to regulate and criminalize the use of deep-fakes in these contexts.

3. ROLE OF SOCIAL MEDIA

Social media is playing a very vital role in both facilitating and preventing cybercrimes. While they help disseminate nasty content, such as revenge porn and harassment, there are times when their content moderation is quite inconsistent. Many platforms have weak policies or rarely respond to complaints, thus leaving the victims exposed.

More stringent moderation practices and more complex legal frameworks are called for to hold these platforms accountable (Marwick & Caplan, 2018). Social media, however, such as Facebook and Instagram, have faced criticism based on their inability to remove harmful content, thus necessitating a better digital safety system and mechanism that provides support to the victims.

LEGAL CHALLENGES

1. INCONSISTENT LEGAL FRAMEWORKS:

India faces significant challenges in cybercrime enforcement, mainly due to the uneven implementation of legal frameworks across various jurisdictions. The Information Technology Act, 2000, acts as the main legislation governing cybercrimes; however, the enforcement of this very statute is lopsided between states. Moreover, the lack of specific provisions to deal with newly emerging offenses, such as cyberstalking and deep-fake technology, leaves loopholes open for offenders to take advantage of. The Indian Penal Code (IPC) offers certain measures of redress through provisions such as Section 354D, which addresses cyberstalking; however, these provisions frequently fall short in addressing the intricate nature of digital offenses (Sharma, 2020). The lack of uniform cybercrime legislation throughout India results in varying judicial interpretations and implementations, thereby hindering victims in their pursuit of justice.

2. DEEP-FAKE REGULATIONS

Deep fake technology, producing manipulated videos or images targeting an individual to exploit for a particular purpose, tends to be a new major threat to women in this regard. India does not currently have comprehensive legal frameworks to deal with the implications of deep-fakes. Specific provisions under the IT Act, 2000, and the IPC might be utilized while dealing with defamation and harassment cases; however, such statutes were drafted without considering deep-fake technology, making the enforcement of such laws challenging (Shroff, 2021). Experts suggest reforms to introduce explicit provisions criminalizing the creation and dissemination of deep-fakes, along with penalties that reflect the seriousness of these offenses. Additionally, legal measures should include mechanisms for quickly removing harmful content from online platforms to protect victims.

3. PROTECTION FOR VULNERABLE WOMEN FROM ONLINE HARASSMENT ON SOCIAL MEDIA PLATFORMS

Consecutively, online harassment of women-especially on social networking sites-is a growing concern in India. Legal safeguards for female victims of harassment are Section 67 of the IT Act, which criminalizes obscenity-based contents transmission, and Section 354A of the IPC related to sexual harassment. However, these acts often lack the potency to seriously address the specific challenges surrounding online social media harassment, such as the speedy spread of harmful content (Kaur, 2019). Amendments to these acts should focus on making social media companies responsible for unfavourable content and improving their effectiveness in removing objectionable content. A clear legal framework should be established that ensures greater protection and effective redressal measures for women online.

ETHICAL CONSIDERATIONS

1. AI AND WOMEN WELFARE

AI technologies have raised many ethics questions, particularly within the Indian context, within the domain of women's protection services. While these technologies hold the capability of increasing

safety through pattern recognition associated with harassment or abuse, they throw up major concerns related to data security, consent, and privacy. Where digital literacy is uneven in India, vulnerable groups of women may not fully understand how data collected by AI is used or shared. An access by AI systems into sensitive personal information without explicit consent creates a possible risk of misuse or unauthorized access and brings concerns about privacy. In addition, the lack of rigorous data protection law in India exacerbates these challenges since the existing frameworks, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have not addressed these specific challenges posed by AI technologies Goyal 2020. Privacy protections need to be further enhanced, and there is also an important need to make individuals aware of the services given by AI technologies.

2. ETHICAL AI DEVELOPMENT

For AI to be ethically developed and deployed, particularly in India, clear guidelines must be established to minimize risks for vulnerable groups, especially women. One key approach is to ensure transparency in AI decision-making processes, so individuals understand how outcomes are generated. Additionally, AI systems should be designed to avoid bias, particularly gender bias, which can perpetuate stereotypes or unfairly target women. Schemes like the NITI Aayog's National Strategy for AI categorically represent how artificial intelligence systems must be born equitable and inclusive, and hence achieving ethical development from the very root (Dahiya, 2021). Ethical standards must be integrated in the development of AI at regular intervals of time with ethical assessments to minimize the potential harm to women as well as other at-risk populations.

3. DIGITAL LITERACY

The importance of digital literacy is to educate these vulnerable women in India regarding the risk factors surrounding technology and AI. Many women in rural India don't have the awareness and skills needed to protect themselves from digital risks like online harassment, identity theft, and data breaches. Therefore, educating women on good and bad online practices, such as understanding the threats from online hackers and how to understand the privacy setting in their electronic devices, is important for responsible online activity. Government programs like PMGDISHA try to empower rural areas of India through the enhancement of their digital literacy by making women confident enough to use the digital framework responsibly (Sharma, 2020). Such proliferations are necessary to develop proper usage of technology among vulnerable groups.

PROPOSED SOLUTIONS

1. LEGAL REFORMS

Currently, the legal system of India needs strong support in order to provide an adequate level of protection against cyber criminality, especially for persons in risk groups, including female and juvenile. Current legal frameworks are still the Information Technology Act of 2000, and therefore there is need to update the laws. The enhancement of such crimes like online harassment, cyberstalking, and child exploitation requires better definitions, and stricter reliable regulations. For example, it

indicated that come up with certain consequences for such offenders can help in reducing cybercrime activities as well as afford better protection to vulnerable populations (Chawla & Soni, 2020).

2. SOCIAL MEDIA ACCOUNTABILITY

Thus, social networks are one of the key sources of transmitting negative messages. India should support political measures that will compel these site to take responsibility of the posts on their websites. Based on proposed legislation then the penalty could be fines or even legal consequences for failure to adhere to such contents moderation policies. This would put pressure of platforms to address problems like hate speech, fake news, and cyberbullies in advance. That is why, for example, the draft of amendments to the IT Act focuses on the need for platforms to take responsibility for users' protection (Sangwan & Singh, 2021). By regulating different sectors, such as technology, government can help users and give them a way to fight against abuses that occur on the internet.

3. PUBLIC AWARENESS AND DIGITAL LITERACY PROGRAMS

It is also critical to enhancing attendance at seminars, workshops and public awareness as well as availing digital tools to the vulnerable groups. Measures should be taken with regard to raising awareness of the targeted population on preventive measures that one should take to be protected from threats present on the Internet, threats identification and the rights that people have online.

A good example of cross-sector collaborations is collaborations with non-government organizations where it is possible to design broad extension education programs for both the urban and peri-urban poor as well as rural poor clientele. For example, seminars with expert presentation, webinars can be introduced to inform users and equip them to defend oneself from probable dangers (Nayak, 2021).

4. GLOBAL COOPERATION

Cybercrime threats are universal, and it is a challenge for different countries to come up with efficient solutions for the problems. India should play a proactive role in international debates and formulations and treaties for elimination of cyber related offenses. Other countries can share intelligence, human and other resources and success stories with India to get the benefits from the country. In its example, engaging in the programmes like Budapest Convention on Cybercrime will help the country to with other police forces globally and improve the country's fight against cyber threats (Jha, 2022). Legalization can also enhance compliance with legal rules and norms to make it very difficult for cross border cyber criminals.

CONCLUSION

The research underscores the pressing issue of cyber crimes against vulnerable groups, particularly women, highlighting a disturbing trend of gender-based harassment in digital spaces. Key findings reveal that the evolution of the internet has not only facilitated communication and connectivity but has also created an environment ripe for cyber abuse. Women face unique risks such as cyberstalking, harassment, and the dissemination of non-consensual images, often exacerbated by societal hierarchies that normalize violence against them. The studies reviewed emphasize the need for a comprehensive

understanding of these issues to effectively combat the systemic problems perpetuating gender-based violence online.

To address these challenges, a multi-faceted approach is essential. Legal reforms must be enacted to strengthen existing frameworks like the Information Technology Act, 2000, ensuring they effectively tackle emerging threats such as cyberstalking and deep-fake technology. Technology companies also bear a responsibility to implement stricter content moderation policies and be held accountable for harmful content on their platforms. Additionally, public education initiatives should focus on enhancing digital literacy among vulnerable populations, empowering individuals with the knowledge and skills needed to navigate online spaces safely.

Furthermore, global cooperation is vital in the fight against cybercrime. As cyber threats transcend national borders, collaboration among governments, tech companies, educators, and civil society is crucial. By sharing resources, intelligence, and best practices, stakeholders can work together to create a safer digital environment for all users, particularly those most at risk.

In conclusion, while the challenges posed by cyber crimes are significant, the combined efforts of legal reform, technological innovation, and education can provide a robust framework for protecting vulnerable groups. Ongoing dialogue and partnership among all stakeholders are essential to fostering an inclusive and secure online space, ensuring that everyone, especially women, can participate in the digital world without fear of harassment or violence.

*****

REFERENCES

- Bates, S. (2017). Cyber harassment in online spaces: Gender differences and impacts on women. *Feminist Media Studies, 17*(3), 363-378.
- Chawla, S., & Soni, R. (2020). Cyber law in India: An analysis of the legal framework. *Journal of Cyber Law, 12*(1), 45-60.
- Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment. .
- Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753-1800.
- Dahiya, S. (2021). AI in India: Ethical development and governance strategies. *Journal of Emerging Technologies in Governance, 3*(2), 45-56.
- Faith, B., & Fraser, E. (2019). Digital harassment of women leaders: A review of the evidence.
- Goyal, A. (2020). AI, privacy, and women protection services: Addressing ethical challenges in India. *Indian Journal of Law and Technology, 16*(4), 78-89.
- Jha, A. (2022). Global strategies against cybercrime: The Indian perspective. *International Journal of Cybersecurity, 14*(3), 77-89.

- Kaur, R. (2019). Online harassment of women: Legal responses and social impacts in India. *Journal of Cyber Law & Policy, 4*(2), 112-127.
- Marwick, A., & Caplan, R. (2018). Drifting through the net: Content moderation, algorithmic practices, and cultural factors in digital spaces. *New Media & Society, 20*(9), 3317-3334.
- Mukherjee, A. (2019). Cyberstalking and the law in India: A critical analysis. *International Journal of Law, 5*(6), 15-25.
- Nayak, P. (2021). Promoting digital literacy in India: Challenges and strategies. *Journal of Educational Technology, 9*(2), 120-135.
- Sharma, R. (2020). Digital literacy initiatives and their impact on rural women in India. *Journal of Digital Empowerment, 5*(1), 33-41.
- Sharma, V. (2020). Inconsistent application of cyber laws in India: Challenges and recommendations. *Indian Journal of Law and Technology, 16*(1), 45-67.
- Shroff, A. (2021). Deep-fake technology and the Indian legal framework: The need for reform. *Indian Law Review, 5*(3), 198-215.
- Simons, N. (2015). Addressing gender-based harassment in social media: A call to action'.

*****

SECURING THE FUTURE: AI-DRIVEN CYBER THREATS, INTERNATIONAL LAW, AND TECHNOLOGICAL DEFENSES

Dr. Fowmina C.[52]

ABSTRACT

The swift progression of artificial intelligence (AI) has profoundly transformed the cybersecurity domain, presenting both improved defensive mechanisms and novel, intricate cyber threats. This study analyses the influence of AI on cybersecurity within the framework of international law and cyber law, emphasising the emerging issues presented by AI-driven cyberattacks, including automated hacking, AI-enhanced malware, and deepfake-related misinformation operations. This article examines existing international legal frameworks, including the Budapest Convention on Cybercrime, and assesses their efficacy in mitigating cross-border AI-related risks, therefore identifying significant regulatory deficiencies. It examines how global collaboration and revised cyber legislation might alleviate the dangers associated with the militarisation of AI. The study also emphasises advanced AI technologies utilised to strengthen cyber defences, such as machine learning for immediate threat identification, AI-augmented encryption methods, and automated incident response. Although these technologies offer improved security, they also provoke ethical dilemmas around privacy, monitoring, and the potential for AI systems to be used by nefarious individuals. This article advocates for a multidisciplinary strategy that synthesises international law, cyber law, and technology to establish comprehensive global governance frameworks. Collaboration among governments, international organisations, and the corporate sector will be essential in guaranteeing that AI bolsters, rather than compromises, global cybersecurity initiatives.

Keywords: AI-driven cyber threats, international law, cyber law, AI-powered malware, deep-fake disinformation, cybersecurity frameworks, and privacy surveillance ethics.

INTRODUCTION

From banking and beyond to healthcare, the rapid advancement of artificial intelligence (AI) has revolutionised industries all around and altered our approach to solve issues and innovation. But alongside this progress comes an equally significant set of challenges, particularly in the realm of cybersecurity. AI is no longer restricted to benign or helpful uses; hackers and state actors are weaponising it more and more to start increasingly complex and catastrophic attacks. The dynamic nature of artificial intelligence along with its ability to learn, adapt, and execute autonomous operations pose a special and growing threat to global digital security.

Rising AI-driven cyber threats are posing additional challenges for governments, businesses, and international organisations into their path. Still essential, traditional cybersecurity methods cannot handle these fresh risks. Artificial intelligence is used by cybercriminals to automate phishing, modify malware, bypass security, and exploit vulnerabilities at speeds and scale never seen in other fields. This growing threat demands a comprehensive, multi-pronged response encompassing not just advanced technological defences but also a solid regulatory framework transcending national borders.

This presentation will explore the effects of AI-driven cyberattacks coupled with the present shortco-

[52] Assistant Dean cum Assistant Professor at Vinayaka Mission's Law School (VMLS), Chennai, India.

mings in international laws and the critical role technology defences play in safeguarding digital infrastructure. Ensuring the future of cyberspace depends on the capacity of global stakeholders to actively confront these evolving threats as the world grows more linked by modifying their legal, ethical, and technical approaches.

THE EMERGENCE OF AI-DRIVEN CYBERTHREATS

Many disciplines, including cybersecurity, where it serves both as a weapon for hackers and a defensive mechanism, are adopting artificial intelligence (AI). The duality of artificial intelligence's impact on cybersecurity shows both its capacity to increase defensive measures and to automate harmful operations as well as to improve their impact. The cybersecurity scenario is changing dramatically as AI gradually pervades the toolkit for bad actors causes new challenges to arise.

AI AS A CYBERCRIME TOOL

Driven by its potential to absorb vast amounts of data, learn autonomously, and immediately adapt to defences, artificial intelligence's arrival into cybercrime has been speeding. Growing availability of artificial intelligence technology has democratised cybercrime, allowing even less technologically capable criminals to deploy advanced AI tools with malicious intent. AI-powered assaults are more difficult to detect and halt since they continually modify their tactics, learn from failures, and create unlike traditional cyberattacks—which often need for human involvement.

ARTIFICIAL INTELLIGENCE-POWERED PHISHING ATTACKS

Long one of the most common types of cyberattacks, phishing has become far less successful using artificial intelligence. Using machine learning to examine personal digital behaviour, AI-driven phishing assaults let attackers create quite tailored and convincing phishing emails or messages. These attacks use natural language processing (NLP) to replicate human communication patterns, therefore rendering them indistinguishable from actual messages, instead than depending on generic, obviously observable attempts. Furthermore widely deployed are phishing campaigns driven by artificial intelligence. Automation helps attackers to send tailored phishing messages to thousands of targets at once, hence greatly raising the probability of success. Since conventional anti-phishing solutions find it difficult to keep up with the fast changing strategies used by artificial intelligence systems, these attacks especially challenge defence against.

DEEPER FAKE TECHNOLOGY AND DISINJURY

Among the most frightening applications of artificial intelligence in cybercrime is deepfake technology. Using artificial intelligence algorithms, deepfakes create hyper-realistic images, sounds, or recordings of humans that may be manipulated to look as though they are speaking or acting in ways they never would have done. From political disinformation operations to corporate sabotage and identity theft, these AI-generated deepfakes might find use in a variety of dark settings.

Deepfakes provide a particular threat in the digital era as they may be weaponised to erode public faith in institutions, undermine elections, or influence the financial markets. Attackers could create a video of a CEO making fake statements aimed to affect stock prices. Likewise, political leaders' deepfake

voices might be used to cause unrest or conflict. Rising complexity of deepfakes increases their difficulty to detect, hence compromising personal privacy and national security.

ARTIFICIAL INTELLIGENCE-ENABLED RANSOMWARE AND HARDWARE

Malware and ransomware attacks have been pillar of cybercrime for years; now, artificial intelligence's presence increases these threats. More successful in escaping traditional detection methods including antivirus software or firewalls, AI-enabled malware may learn from its environment and change its behaviour in real-time. Behavioural studies suggest that AI-powered ransomware might autonomously target vulnerable systems, then forecast which victims are most likely to pay ransoms.

Moreover, artificial intelligence makes it possible for the assault process to be constantly better. By means of analysis of the defences of various systems, artificial intelligence algorithms may change the malware to exploit specific weaknesses, therefore promoting continuous development. These adaptive characteristics guarantee that the virus may grow to remain effective even after discovery, beyond traditional cybersecurity measures.

AUTOMATED EXPRESSIVE LEARNING

One of the most deadly applications artificial intelligence is weaponised in cybercrime is automation of vulnerability screening and exploitation. Autonomously searching large datasets, networks, or systems for security concerns, artificial intelligence algorithms might identify potential assaults far faster than human capacity. Once problems are found, artificial intelligence might develop vulnerabilities and launch attacks on its own free will without human control.

With this degree of automation, attackers may target individuals, businesses, or governments indiscriminately then locate and exploit weaknesses on a mass basis. The development of artificial intelligence in these environment suggests that hostile actors can uncover and exploit even zero-day vulnerabilities—those heretofore unknown to the security community—before solutions can be developed.

ARTIFICIAL INTELLIGENCE DRIVEN BOTNETS AND DDOS ATTACKS

More notably, artificial intelligence is enabling distributed denial-of- service (DDoS) attacks—which flood systems with a tsunami of internet data to compromise services. Operating more efficiently than traditional botnets, AI-driven botnets on their own autonomously manage and control thousands, perhaps millions, of infected devices. More strong against countermeasures, these AI-driven bots might change their attack strategies right away.

By alternating many attack strategies, machine learning models in AI-powered DDoS attacks may predict the most vulnerable periods for assaulting or even circumvent defence measures. These very effective AI-driven DDoS strikes have size and accuracy that reflect their impact against well-known websites, financial institutions, and important infrastructure.

THE WEAPONISING OF ARTIFICIAL INTELLIGENCE: A THREAT RISING

As cybercriminals weaponise artificial intelligence, there becomes increasing likelihood of large, automated cyberattacks. Artificial intelligence reduces the entrance barrier for cybercrime by letting

attackers attain before unheard-of efficiency, scale, and complexity, therefore enabling even small threat actors to launch complex operations.

ARTIFICIAL INTELLIGENCE FOR CYBER CRIME

Moreover, artificial intelligence turns into a helpful tool for cybercrime. State-sponsored spies are using artificial intelligence increasingly for information gathering and surveillance. Given national security, where AI-driven cyber espionage might expose military and sensitive government data, these capabilities truly concern me. Through massive data processing, network infrastructure mapping, and target identification for exploitation, artificial intelligence systems can map entire networks, extract useful information,

AI is the ideal tool for identifying high-value targets as its ability to examine vast amounts of data enables it to identify trends and relationships people would overlook. Artificial intelligence might be used in the realm of espionage to automatically break through systems, intercept communications, and exfiltrate data without leaving any trace.

SYSTEMS OF INDEPENDENCY ATTACK

One of the most worrying developments in weaponising is rising autonomous attack systems. artificial intelligence. These devices might launch cyberattacks under human controllessness and make real-time decisions based on the surroundings. Based on the target, autonomous attack systems can change their behaviour; they can dodge defences, even self-replicate across networks, thereby dispersing from system to system with least human participation.

From financial systems to healthcare networks to power grids, autonomous AI-driven attacks significantly threaten critical infrastructure. Especially if they target basic utilities, these systems might cause great disturbance, financial damage, and even death if let uncontrolled. Within the field of cybersecurity, the rise of artificial intelligence-driven cyberthreats signals a radical transition. While artificial intelligence may be a tool for good, its weaponising by state actors and cybercriminals generates a range of new risks testing the capacity of conventional measures to be offset. From adaptive malware and autonomous attack systems to AI-powered phishing assaults and deepfakes, the geography of cyber hazards is rapidly shifting. If governments, companies, and cybersecurity professionals are to protect against these escalating threats, they must remain ahead of the curve by building advanced technical defences and applying forward-looking legislative frameworks. Modern technology, global cooperation, and a commitment to ethical AI research will all be part of securing the future as artificial intelligence keeps altering the landscape of cybersecurity.

INTERVENTIONS IN INTERNATIONAL LAW AND CYBERSECURITY: CHALLENGES AND GAP

As artificial intelligence-driven cyber threats evolve, the difficulty of designing legal structures to manage these growing hazards becomes evident for the world community. Cyberattacks cross national lines as they impact governments, businesses, and individuals all across the world. While efforts to regulate cyberwarfare and cybercrime have progressed, the rapid speed of technology development has

exposed fundamental flaws in the present global legal framework. These restrictions make it difficult to hold perpetrators accountable, combat cyberattacks, and worldwide protect vital infrastructure.

This section will address the current state of international law in relation to cybersecurity, the challenges in changing legal frameworks to manage AI-driven cyberthreats, and the great need of global collaboration to establish more effective legal procedures. Comparatively to other sectors like air, land, and sea, international law regulating cyberspace is still in infancy. The Legal Framework of Today for Cybersecurity. Notwithstanding several bilateral and international agreements aimed to enhance cybersecurity, the legal systems managing cyberthreats remain disconnected and occasionally out of current. The challenge is the fast-paced, anonymous, often hard to connect to a particular actor or state character of cyber activity.

THE MANUAL ON TALLINN

Among the most notable projects aiming at creating a legal foundation for cyberwarfare is the Tallinn Manual on the International Law Applicable to Cyber Warfare. Under guidance of the NATO Cooperative Cyberference Centre of Excellence, the Tallinn Manual provides a review of how modern international laws—including the United Nations Charter and the Geneva Conventions—apply to cyber operations during armed conflict. This is the output of a group of professionals.

The Tallinn Manual is a great tool for governments and businesses managing the legal complexity of cyberwarfare even if it is not legally enforceable. It shows that, under international humanitarian law (IHL), which regulates conduct during wars, internet activities also fit. During armed conflict, IHL outlaws cyberattacks targeted at civilians or civilian infrastructure (such as hospitals or water supply).

But the Tallinn Manual addresses cyber operations within the realm of armed conflict alone. Especially in situations involving AI-driven attacks, it provides inadequate comprehensive guidance for peacetime cyberattacks. Still a big hole is the absence of legally enforceable international laws regulating peacetime cyberspace operations involving economic harm, cyber espionage, and disinformation campaigns.

Adopted in 2001, the Budapest Convention on Cybercrime is another significant worldwide legal instrument aimed to combat cybercrime. It seeks to unify national laws, improve investigative techniques, and support global cooperation against cyberscrime. Among the numerous forms of cybercrime addressed under the Budapest Convention are unauthorised access to computer systems, data breaches, and virus use.

While more than 65 countries have joined the Budapest Convention, other powerful players—including China and Russia—have refused to sign it claiming concerns about sovereignty and potentially Western powers' prospective abuse. This refusal to join a common cybercrime framework limits worldwide attempts to battle cyber threats as cybercriminals may exploit countries that do not support international investigations.

Moreover, the Budapest Convention was draughted long before cyberattacks powered by artificial

intelligence started to show up and so does not especially address the use of artificial intelligence in cybersecurity. As artificial intelligence is being weaponised in phishing, ransomware, and botnet attacks, the convention has to be changed to reflect these mounting risks.

Jurisdictional and Attribution Problems: Implementing international cybersecurity legislation is hampered most importantly by the attribution question. Cyberattacks are notably difficult to connect with certainty as attackers may easily disguise their identity, utilise proxies, or operate across foreign networks. This ambiguity makes it difficult to hold perpetrators accountable, especially in circumstances when the attack involves autonomous AI-driven systems or criminals under government sponsorship.

Whether by military responses, civil action, or penalties, enforcement of legal duty relies on attribution in determining attackers. Still, the nature of cyberattacks makes attribution exceedingly challenging. Attacks driven by artificial intelligence, for instance, may originate anywhere in the world and be difficult to follow their origin. Attackers can also utilise artificial intelligence to copy the behaviour of other players, therefore creating confusion on who is responsible.

Especially problematic are state-sponsored attacks as governments can refuse involvement and claim that unaffiliated hackers carried out the strikes. Given this ambiguity, the international community struggles to sanction countries engaged in cyber espionage, sabotage, or attacks on important infrastructure.

Jurisdictional problems offer still another major legal barrier. Often involving numerous countries, cyberattacks involve victims, offenders, and compromised systems dispersed over several countries. This raises challenging legal questions about whether country has authority to investigate and punish the crime. An artificial intelligence-driven botnet, for example, may compromise devices across many countries and carry coordinated attacks on important infrastructure in a rather different jurisdiction, so the issue is much more complex when AI-driven attacks span borders since AI systems may independently run across several nations without human control. Selecting which country should seek legal action under which guidelines can become a logistical and legal headache, generally postponing or preventing rapid fixes.

Particularly the concepts of distinction, proportionality, and necessity, the increasing use of artificial intelligence in cyberwarfare also presents novel challenges for the application of international humanitarian law (IHL), in accordance with armed conflict rules. Basic to the guidelines of armed conflict, these concepts demand that combatants differentiate military from civilian targets, that attacks be proportional with their military advantage achieved, and that they be obliged to fulfil a reasonable military purpose.

Artificial intelligence-driven cyberattacks blur the military from civilian targets, therefore separating them. Unlike traditional warfare in which military facilities and soldiers are clearly recognised, cyberattacks usually target dual-use infrastructure such communication networks, power grids, and financial institutions, which serve both civilian and military purposes. AI systems—especially those operating autonomously—may find it challenging to differentiate between civilian infrastructure and

approved military targets, therefore raising issues of IHL compliance. An artificial intelligence-powered strike aiming to compromise a nation's military communication network, for example, may inadvertently damage civilian lines of communication, therefore compromising the civilian population. Although the intended aim was military assets, such incidents might be considered as IHL violations.

Based on the proportionality principle, harm done to civilian property or persons during an attack cannot be too severe in regard to the projected military advantage. In the scope of AI-driven attacks, especially when the attack is carried out by an autonomous system able of continuous method evolution, determining proportionality becomes ever more difficult. While AI systems could be taught to achieve certain objectives, they may unintentionally do too much damage during their lifetime.

Likewise, the necessity principle insists that attacks be limited to what is absolutely essential to achieve a reasonable military purpose. Conversely, autonomous artificial intelligence systems may have unexpected consequences and increase attacks above what is needed. Targeting a military station first, an AI-driven system can then broaden the attack to civilian networks, therefore violating the idea of need as part of their self-learning process. Given the global dimension of AI-driven cyberthreats, effective cybersecurity governance demands for international cooperation. Lack of a clear international strategy for cybersecurity and artificial intelligence control impedes efforts to address these issues. Though regional agreements—like the General Data Protection Regulation (GDPR) of the European Union and cybersecurity policies accepted by individual countries—the lack of a comprehensive, legally enforceable international convention on artificial intelligence and cybersecurity causes substantial gaps.

SETTING GUIDELINES FOR RESPONSIBLE STATE ACTION

One of the first steps in addressing AI-driven cyber threats is defining international norms for responsible state activity in cyberspace. Under initiatives of the Open-Endered Working Group (OEWG) and the United Nations Group of Governmental Experts (UNGGE), voluntary guidelines for state behavior—such as avoiding attacking key infrastructure during peacetime—have sought development.

Although these guidelines are not legally binding, should governments violate them there is no way to make them responsible. Especially in connection with AI-driven attacks, the global community has to focus on the draughting of legally enforceable agreements setting precise rules for state activity in cyberspace.

b) promoting global collaboration and knowledge sharing Especially those including artificial intelligence, cyber hazards may crop up rapidly and might do great damage before they are fully known. Strengthening international collaboration and information-sharing networks among law enforcement agencies, business sector corporations, and countries can help to allay these issues. Although regional entities like the European Union and ASEAN have moved to improve cybersecurity cooperation, a more coordinated worldwide strategy is needed since cooperation helps to better the attribution of attacks, speed up reaction to assaults, and enable the sharing of best practices for resisting artificial intelligence-

driven threats. This might include the development of global norms, an international organisation monitoring artificial intelligence-driven cyberthreats, and global reaction to significant breaches.

For international law and cybersecurity governance, the development of AI-driven cyber threats presents heretofore unheard-of challenges in managing the complex legal environment. Although helpful, the present legal structures are not suited to manage the complete spectrum of these recently developing threats. The challenges in attributing cyberattacks, the lack of clear jurisdictional limitations, and the application of traditional principles of international humanitarian law to AI-driven assaults lead to a convoluted legal environment.

The international community has to provide the legally enforceable agreements notably addressing AI-driven cyber hazards high priority moving forward. This will demand for technical inventiveness, political endeavours, and global improvement.

CHANGING TECHNOLOGY DEFENCES AGAINST AI-DRIVEN THREATS

The defences that guard sensitive data, personal privacy, and vital infrastructure must change along with the evolving AI-driven cyberthreats Conventional cybersecurity techniques are insufficient as malevolent actors use artificial intelligence to undertake complex assaults. The evolution of sophisticated technical defences that use artificial intelligence, automation, and machine learning to forecast, identify, and neutralise threats in real-time will define cybersecurity going forward. The main technology developments arising in response to AI-driven cyber threats will be discussed in this part Among these changing defences are automated incident response, quantum-resistant encryption, threat detection driven by artificial intelligence, and the increasing relevance of cooperation between cybersecurity professionals and artificial intelligence researchers. These technologies taken together reflect the future of cybersecurity, in which artificial intelligence's capabilities affect both offensive and defensive strategies ever more.

One should start by Development of AI-powered detection systems that can spot harmful behaviour before it does major damage is the first line of protection against AI-driven cyberthreats. Firewalls, antivirus programs, and signature-based detection are among the conventional cybersecurity tools that find it difficult to match the speed and complexity of assaults enabled by artificial intelligence. But new opportunities for danger identification and prevention abound from machine learning and artificial intelligence technology.

Particularly successful in identifying abnormalities in network traffic and user behavior—which can indicate a possible cyberattack—are machine learning for anomaly detection AI systems. By means of large datasets, machine learning algorithms may be taught to create a baseline of typical behaviour for a certain network or system. Once the artificial intelligence (AI) knows what "normal" looks like, it can rapidly spot variations that can point to a phishing effort, malware, or infiltration. An AI-powered system may, for instance, track employee activity on a company network, examining login patterns, data access, and file transfers. Should an employee's account show unusual activity—such as accessing private information at odd hours or starting a significant data transfer—the system would flag the

conduct as suspicious and start additional inquiry or containment actions. Though the assault path has not been known before, this kind of anomaly detection enables proactive threat identification.

By means of predictive modelling, predictive threat modelling artificial intelligence may also help to foresee upcoming cyber dangers. Through the analysis of past attack trends, artificial intelligence systems can project where and how future assaults could take place, therefore allowing companies to strengthen their defences in line. Because these prediction models learn constantly from fresh data, they may change with changing attack plans. AI models might find, for example, that ransomware assaults are progressively focussing on particular kinds of companies, including banking institutions or healthcare providers. Then, depending on the changing threat environment, the system might send notifications to these companies suggesting certain security precautions.

Additionally enhancing authentication methods are behavioural biometrics and continuous authentication systems driven by artificial intelligence. An extra layer of protection can come from behavioural biometrics—which examine distinctive patterns in how people interact with devices—e.g., typing speed, mouse motions, or mobile gestures. Real-time analysis of these actions by artificial intelligence systems constantly checks that the individual engaging with the system is truly the authorised user. Behavioural biometrics are far more difficult for attackers to imitate than more conventional authentication techniques include passwords or even biometrics like fingerprints. Should an illegal user find their way onto a system, the artificial intelligence will identify the behavioural differences and respond right away, maybe logging the user off or alerting security staff.

One of the most important difficulties in contemporary cybersecurity is automated incident response and recovery considering the pace of threat development. Particularly AI-driven dangers can start and spread quicker than human reactions allow. Organisations are thus looking to artificial intelligence more and more for automated incident response and recovery solutions that can neutralise threats in real-time, therefore lessening the effect of successful assaults. Response speed is crucial in real-time response automation should a cyberattack be discovered. When AI senses a danger, it may be taught to automatically perform specific tasks as isolating compromised accounts, disabling hacked equipment, or blocking hostile IP addresses. This real-time reaction capacity guarantees that the assault is limited before it may reach other areas of the network or inflict major harm. In the case of a ransomware attack, for instance, an AI-driven response system may instantly identify file encryption, separate the impacted computer from the network, and start a backup recovery effort. AI-driven systems can minimise assault damage and stop mass data loss by moving faster than human responses.

Threat feeds, social media, and the dark web are just a few of the data sources from which threat intelligence platforms driven by artificial intelligence may compile and evaluate. This data then helps to provide a whole picture of new dangers, enabling companies to give the most urgent concerns top priority and react accordingly. From recording events to creating reports for security teams, incident management solutions leveraging artificial intelligence may automate much of the incident response process. This lessens the work for human analysts, who may then concentrate on more strategic chores include evaluating difficult risks or creating long-term security plans.

One often used vulnerability by hackers is obsolete software with unpatched security weaknesses. AI can apply fixes over vast networks and automate vulnerability detection. Automating this approach helps companies greatly narrow the window of opportunity for attackers to take advantage of identified weaknesses. Furthermore, depending on the degree of the vulnerability and the importance of the impacted systems, artificial intelligence may rank fixes. This guarantees that the most urgent security issues are taken care of first, therefore lowering the possibility of effective assaults.

As AI-driven attacks becoming more sophisticated, the introduction of quantum computing presents another challenge to conventional encryption techniques. Widely used encryption systems as RSA and ECC (Elliptic Curve Cryptography) might be broken by quantum computers, therefore exposing most of the sensitive data in the globe to decode. Researchers are creating quantum-resistant cryptography algorithms able to resist the computing capacity of quantum computers in order to handle this increasing risk.

Post-quantum cryptography is the field of security-oriented encryption techniques meant to withstand attacks from both conventional and quantum computers. Development and testing of many post-quantum cryptography techniques are under way in an attempt to create new standards capable of substituting for current encryption systems before quantum computers become generally accessible. AI may be quite important in controlling quantum-resistant cryptography systems going forward. Based on the particular threat environment, AI-driven systems might automatically alternate between many encryption techniques, therefore assuring that critical data is encrypted even if new quantum capabilities develop.

b) AI-Driven Cryptographic Solutions AI itself may also be applied to bolster cryptographic systems. Machine learning techniques, for example, may be used to find flaws in cryptography implementations, therefore enabling companies to strengthen their encryption systems prior to attack exploitation. Furthermore able to maximise encryption techniques is artificial intelligence, which guarantees effective application of cryptographic safeguards throughout extensive systems without compromising speed.

Security Operations Centres (SOCs) have to manage an excessive volume of data and warnings as cyberattacks becoming more frequent and complicated. By supplementing human analysts, automating monotonous operations, and offering deeper insights into possible threats, artificial intelligence might improve the capacities of SOCs.

One of the main difficulties SOCs have is the enormous amount of warnings produced by different security tools: artificial intelligence for threat prioritising Many of these false positives cause alert tiredness in human analysers. By sorting and prioritising warnings, artificial intelligence can assist to guarantee SOC analysts concentrate on the most important risks. By examining trends and relationships between several alarms, machine learning algorithms identify which ones most likely depict real dangers. This procedure greatly lessens the burden for security staff and enhances SOC general performance. By use of data correlation from several sources, AI-powered systems may also offer a more complete picture of an assault, therefore enabling analysts to grasp the whole extent of

the danger and respond more successfully.

AI-driven security analytics systems can rapidly evaluate enormous volumes of security data in real-time, identifying hidden risks that would be difficult for human detection by hand. Using sophisticated algorithms, these systems examine system logs, user behaviour, and network traffic to find trends suggesting a stealthy or slow-moving attack—that is, an advanced persistent threat (APT.). AI-driven analytics give SOCs a strong weapon to find and neutralise attacks early in the attack life by always observing for suspicious behaviour and seeing possible hazards before they get more severe.

Cooperative Defence: The Value of Human Expertise and AI Though AI is not a magic bullet, it is very vital in protecting against cyberattacks. Good cybersecurity calls for human knowledge and powerful AI-driven technologies. Professionals in cybersecurity offer context, intuition, and strategic thinking not replicable by artificial intelligence systems. Working together, artificial intelligence and human analysts can build a stronger defence against changing threats.

Making strategic choices and evaluating the results of AI systems depend on human cybersecurity experts, so they are indispensable. While artificial intelligence may be great at spotting trends and anomalies, human analysts are more suited to grasp the larger background of an assault including the goals and powers of the threat actor. More educated responses to cyberattacks are made possible by this cooperation, especially in complicated settings where artificial intelligence could find it difficult to make complex judgements.

Constant Learning and Adaptation: Cybersecurity is a sector that is always changing and AI systems have to be always upgraded to be useful. To remain accurate, machine learning models need access to the most recent threat intelligence; so, this process is strengthened when cybersecurity experts comment on the performance of the artificial intelligence. Organisations may make sure their defences change in line with the threat environment by include human perspectives on the learning process of the artificial intelligence.

CONCLUSION

Rising AI-driven cyber threats provide governments, companies, and people all around a special and difficult problem. Coordinated, proactive defence techniques are desperately needed as hackers and state actors weaponise artificial intelligence to execute advanced assaults. Although improved technological defenses—such as quantum-resistant encryption and AI-powered threat detection—are very vital in countering these dangers, the fight cannot be won by technology alone.

Future of cyberspace depends on international cooperation and governance. Shared worldwide cybersecurity rules, ethical guidelines for artificial intelligence research, and binding international agreements help to present a cohesive front against hostile actors. Building resilience across sectors and countries will depend critically on public-private partnerships wherein governments and businesses cooperate to exchange knowledge, create new technologies, and react to challenges. Reducing vulnerabilities and building a safer, more secure digital world also depend on encouraging a worldwide cybersecurity ecosystem that enables all countries, regardless of their technological

capacity.

Looking ahead, the world community has to give cooperation top priority over rivalry, cooperation over isolation, and ethical growth over careless invention. By means of these combined initiatives, we can reduce the dangers associated with AI-driven cyber threats, foster confidence in AI technology, and guarantee that cyberspace stays a safe and open venue for creativity, communication, and economic development.

The future of cybersecurity rests not in the hands of one technology or country but in the combined efforts of a worldwide society dedicated to cooperate for the shared benefit. Embracing cooperation and governance as guiding concepts will help us to safeguard the future of our digital environment and shield the planet from the changing risks caused by artificial intelligence.

BIBLIOGRAPHY

1. Budapest Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185.
2. Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2d ed. 2017).
3. U.N. G.A., *Report of the Group of Governmental Experts on Advancements in Cyberspace*, U.N. Doc. A/70/174 (July 22, 2015).
4. U.N. Sec. Council, *Resolution 2341: Protection of Critical Infrastructure*, U.N. Doc. S/RES/2341 (Feb. 13, 2017).
5. General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
6. North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017).
7. *Cybersecurity and Cybercrime: Convention on Cybercrime (Budapest Convention)*, Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
8. John P. Carlin, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (2018).
9. Mieke Eoyang et al., *AI & National Security: The Importance of AI and Cybersecurity for International Security*, *Brookings Inst.* (Oct. 15, 2020), https://www.brookings.edu/research/ai-cybersecurity-and-national-security/.
10. Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 *Calif. L. Rev.* 1753 (2019).
11. International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2020*, *ITU*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.
12. *FireEye Threat Intelligence Reports*, *FireEye*, https://www.fireeye.com/current-threats.html.

*****

THE INFLUENCE OF DEEPFAKE TECHNOLOGY AND ASSOCIATED ETHICAL DILEMMAS

Oindrilla Ghosh[53] and Binod Kumar[54]

ABSTRACT

Deepfake technology, characterized by its ability to generate realistic and compelling digital content through machine learning and artificial intelligence, has rapidly emerged as a significant disruptor in various sectors, including the media, entertainment, and politics. While it presents certain innovative opportunities for creativity and storytelling, deepfake technology also raises substantial ethical concerns. This study explores the multifaceted influence of deepfake technology, emphasizing its applications and the consequent ethical dilemmas it introduces. The capability to fabricate images, audio, and video with high fidelity can lead to the erosion of trust in digital media, making it increasingly challenging for individuals and organizations to discern truth from fabrication. Misinformation, manipulation, and the potential harm to individuals' reputations are pressing issues that demand attention. The ethical challenges extend beyond misinformation; they include questions of consent regarding the use of one's likeness, privacy violations, and the potential for deepfake content to perpetuate harmful stereotypes. Furthermore, governance and regulatory frameworks are lagging, creating a significant gap in addressing these issues effectively. This paper argues for a comprehensive ethico-legal framework that should guide the development and deployment of deepfake technologies, advocating for greater transparency, accountability, and collaborative efforts among stakeholders. Ultimately, while deepfake technology can be harnessed for positive outcomes, an informed and proactive approach is crucial to mitigate its risks and ensure that it does not undermine societal trust or ethical standards.

Keywords: Deepfake Technology, Ethical Dilemmas, Misinformation, Privacy Violations, Consent and Trust

Introduction

Deepfake technology has emerged as one of the most advanced and potentially disruptive applications of artificial intelligence (AI) in recent years. By utilizing sophisticated algorithms and machine learning techniques, deepfakes can create hyper-realistic media that can forge the appearance and voice of individuals, making it increasingly difficult for audiences to distinguish between reality and fabrication. As the technology becomes readily accessible and more sophisticated, its implications span a multitude of domains, including politics, entertainment, law enforcement, and personal relationships. This research article delves into the influence of deepfake technology, exploring its applications, societal impact, and the ethical dilemmas it engenders.

Definition and Mechanism:

Deepfakes are synthetic media in which a person's likeness is digitally manipulated to impersonate someone else. The term "deepfake" itself is a portmanteau of "deep learning" and "fake." The fundamental technology relies on deep learning models, particularly Generative Adversarial Networks (GANs), which consist of two neural networks, a generator and a discriminator, that work in tandem. The generator creates fake images or videos, while the discriminator evaluates their authenticity.

[53] Research Scholar at School of Law, Christ (Deemed To Be) University, India.
[54] Student at School of Law, Shri Venkateshwara University, India.

Through repeated iterations, both networks improve, leading to the production of highly convincing media.

APPLICATIONS OF DEEPFAKE TECHNOLOGY

Deepfake technology finds application in various fields, including:

1. Entertainment and Film: Filmmakers utilize deepfake techniques to enhance visual effects, resurrect deceased actors, or create realistic body doubles. Notable films have incorporated deepfake technology to bring historical figures or CGI characters to life.

2. Political Disinformation: The political ramifications of deepfakes became evident during election cycles, where manipulated videos could misrepresent candidates, spread misinformation, or undermine trust in democratic institutions. A deepfake of a politician delivering controversial statements could sway public opinion and influence electoral outcomes.

3. Security and Surveillance: In law enforcement and security sectors, deepfakes can be weapons for criminals, who can use them to fabricate evidence or create alibis. Conversely, authorities could leverage similar technologies to analyze potential threats or track criminal activity.

4. Social Media and Influencer Marketing: The proliferation of deepfake technology has altered the landscape of social media. Users can create engaging content that leverages the personas of famous figures or generate personalized marketing messages, pushing the boundaries of content creation.

5. Education and Training: Deepfake technology can be employed in educational sectors to simulate scenarios, such as historical reenactments or medical training, allowing for immersive learning experiences.

The societal impact of deepfake technology is multifaceted, leading to both positive and negative outcomes, making its influence increasingly apparent.

Positive Aspects:

1. Enhanced Creativity: Deepfakes offer unprecedented opportunities for creative expression, allowing artists and storytellers to experiment with new forms of media. They foster innovation in filmmaking, video games, and visual art.

2. Personalized Experiences: Users can leverage deepfake technology to create personalized messages, greetings, and memorable moments by superimposing their face onto their favorite film characters or celebrities.

3. Therapeutic Applications: In the realm of mental health, deepfake technology provides potential therapeutic benefits. For example, patients with phobias can be exposed to virtual scenarios that employ a familiar figure, helping to ease anxiety in a controlled setting.

Negative Consequences:

1. Misinformation and Trust Erosion: The most pressing threat from deepfake technology is the potential for spreading misinformation. The capability to manipulate video evidence undermines our collective ability to discern truth from falsehood, fostering a culture of skepticism regarding media.

2. Cyberbullying and Harassment: Deepfake technology can amplify the harm of cyberbullying by creating malicious, fabricated content. Individuals' identities can be distorted, leading to reputational damage, emotional distress, and harassment.

3. Political Manipulation: As political campaigns become more polarized, the potential for using deepfake technology to manipulate public perception rises. The creation of misleading content can erode trust in leaders, media outlets, and democratic processes.

4. Legal and Ethical Boundaries: The insidious nature of deepfakes raises important legal questions around consent, copyright, and attribution. Cases of non-consensual deepfake pornography have emerged, raising issues of agency over one's own likeness.

Ethical Dilemmas:

The exploration of deepfake technology inevitably leads to significant ethical dilemmas as society grapples with its implications. These mainly revolve around issues of consent, authenticity, accountability, and potential regulation.

1. Consent and Privacy: One of the central ethical concerns regarding deepfakes revolves around the issue of consent. Individuals whose images or voices are manipulated often have not given permission for their likenesses to be used. This raises serious questions about personal agency and autonomy. Non-consensual deepfakes, particularly in the realm of pornography, are increasingly prevalent. Victims of such technologies face severe psychological distress, reputational harm, and privacy infringements. The inability to control one’s own likeness in a public domain raises significant ethical questions on the right to privacy and the regulation of digital media.

2. Authenticity and Truth: Deepfake technology poses fundamental challenges to the very notions of authenticity and truth. As media becomes more artificial, discerning fact from fiction becomes increasingly difficult. This can lead to a societal environment where trust in visual media is severely compromised, raising concerns about the moral responsibilities of creators and consumers. Should media platforms be held accountable for facilitating the distribution of deepfakes? The ethical responsibility of both consumers and creators in determining the authenticity of the media they consume and produce looms large.

3. Accountability and Responsibility: The question of accountability surfaces prominently in discussions surrounding deepfake technology. As the line between reality and fabrication blurs, who should be held responsible for the consequences of deepfakes? Is it the creators, the platforms that host the content, or the users who share it? Legal frameworks lag behind technological advancements, resulting in a significant accountability gap. This raises critical ethical considerations regarding how society can effectively navigate the challenges posed by misinformation and identity manipulation.

4. Regulation and Governance: Given the significant ethical dilemmas posed by deepfake technology, the necessity of regulation has become apparent. Policymakers face the challenge of crafting laws and regulations that balance innovation with protection. Any intervention must strike a balance between preventing misuse while not stifling technological development or infringing on free

speech. Potential solutions may involve implementing stringent guidelines for using deepfake technology, introducing penalties for malicious uses, and developing robust reporting mechanisms for victims of deepfakes.

STRATEGIES FOR MITIGATING DEEPFAKE RISKS

As deepfake technology continues to evolve, it is crucial to develop strategies that can mitigate its risks while maximizing its benefits. The following avenues may be explored:

1. Education and Awareness: Increasing public awareness about deepfake technology and its implications can help foster critical media literacy skills. Educating individuals on how to identify deepfakes and encouraging skepticism when encountering dubious media can serve as a first line of defense against misinformation.

2. Technological Solutions: The development of technology capable of detecting deepfakes is crucial in combating the challenges posed by synthetic media. Researchers are actively designing algorithms that can detect discrepancies between real and manipulated media. As detection technology advances, it can reduce the prevalence of harmful deepfakes.

3. Collaborative Efforts: Addressing the challenges posed by deepfake technology requires collaborative efforts among tech companies, government agencies, and civil society. Platforms hosting video content should implement robust policies to prevent the dissemination of malicious deepfakes while promoting transparency and accountability.

COMPREHENSIVE ETHICO-LEGAL FRAMEWORK FOR DEEPFAKE TECHNOLOGIES

As deepfake technologies become increasingly sophisticated and accessible, their potential for misuse poses significant ethical and legal challenges. To ensure responsible development and deployment, a comprehensive ethico-legal framework is essential. This framework should encompass the principles of accountability, transparency, consent, harm reduction, and education.

1. Accountability: The development and deployment of deepfake technologies must prioritize accountability at all levels. Developers, companies, and users should bear responsibility for the implications of their technologies. Legal frameworks should enforce strict penalties for malicious use, such as creation of deceptive content intended to defame, manipulate, or harm individuals or groups. By establishing clear liability for harmful uses of deepfakes, stakeholders will be incentivized to deploy their technologies ethically.

2. Transparency: Transparency is crucial to fostering public trust in deepfake technologies. Developers should provide clear disclosures regarding the capabilities and limitations of their systems as well as the instances in which they've been employed. This could include watermarking deepfake content to signify alterations and ensure that audiences are aware they are viewing manipulated media. Such measures can deter deceptive practices and help viewers critically assess the credibility of the content they encounter.

3. Consent: Informed consent should be a cornerstone of any ethical framework governing deepfake technologies. Individuals should retain control over their likeness and personal data. Any

generation of deepfakes that features a person's image, voice, or other identifying characteristics must require explicit consent from that individual, particularly in contexts like entertainment or marketing. Institutions could establish guidelines outlining how consent should be obtained and documented, ensuring that individuals understand how their data may be used and are able to opt out easily.

4. Harm Reduction: The potential for deepfakes to cause social, psychological, and reputational harm necessitates proactive measures to mitigate such risks. Developers and platforms facilitating deepfake technologies should implement robust content moderation practices. This could involve the use of advanced detection algorithms, user reporting mechanisms, and the establishment of an oversight body to evaluate contentious content. In addition, proactive outreach and harm reduction initiatives should prioritize vulnerable groups such as women, minorities, or public figures to protect them from targeted harassment or misinformation.

5. Education: Finally, public education is essential in equipping individuals to navigate a landscape increasingly filled with manipulated media. Educational initiatives should focus on enabling critical media literacy, helping individuals discern legitimate content from deepfake technologies. Collaboration with educational institutions, non-profits, and tech companies can facilitate the creation of comprehensive curricula that highlight the techniques of discernment and the ethical implications surrounding deepfakes. Raising public awareness can mitigate the potential for misinformation and empower audiences to defend against manipulation.

In an age where the boundaries of reality and fiction can be easily blurred, a comprehensive ethico-legal framework for deepfake technologies is not only necessary but urgent. By embedding principles of accountability, transparency, consent, harm reduction, and education into the development and deployment of these technologies, society can harness their potential while protecting individuals and communities from their misuse. The challenge lies not just in technological advancement but in crafting a governance structure that aligns ethical considerations with legal imperatives, ensuring a balanced approach toward innovation and societal well-being.

CONCLUSION

Deepfake technology represents a remarkable advancement in the field of artificial intelligence and visual media, with applications that hold promise for creativity, education, and entertainment. However, the ethical dilemmas it poses are equally significant, spanning issues of consent, authenticity, and accountability. As society grapples with these challenges, it is essential to adopt a multifaceted approach that includes public education, technological solutions, collaborative efforts, and robust legal frameworks. Only through a comprehensive understanding of the implications of deepfake technology can we navigate the fine line between harnessing its potential for positive uses while safeguarding against its dangers. The road ahead is complex, necessitating ongoing dialogue among stakeholders to address the multifarious concerns posed by this unprecedented technology.

*****

REFERENCES

- Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K. & Li, H. (2019). Protecting world leaders against deep fakes. *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 38–45
- Bound Alberti, F. (2017). From Face/Of to the face race: The case of Isabelle Dinoire and the future of the face transplant. *Medical Humanities*, 43, 148–154.
- Caplan, A. (2004). Facing ourselves. *American Journal of Bioethics*, 4(3), 18–19.
- Caporusso, N. (2021). Deepfakes for the good: A benefcial application of contentious artifcial intelligence technology. Proceedings of the AFHE 2020 virtual conferences on software and systems engineering, and artifcial intelligence and social computing, July 16–20, 2020 (pp. 235–241). *Springer*.
- Carosella, E. D., & Pradeu, T. (2006). Transplantation and identity: A dangerous split? *Lancet*, 368(9531), 183–184.
- Chawla, R. (2019). Deepfakes: How a pervert shook the world. *International Journal of Advance Research and Development*, 4(6), 4–8.
- Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, 49, 345–391.
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1819.
- Diakopoulos, N. & Johnson, D. (2020). Anticipating and addressing the ethical implications of deepfakes in the context of elections. *New Media & Society*, 1–27.
- Edgar, A. (2009). The challenge of transplants to an intersubjective established sense of personal identity. *Health Care Analysis*, 17, 123–133
- Farwell, J. P., & Rohonzinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40.
- Figueira, A., & Oliveira, L. (2017). The current state of fake news: Challenges and opportunities. *Procedia Computer Science*, 121, 817–825.
- Fletcher, J. (2018). Deepfakes, artifcial intelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal*, 70, 455–471.
- Floridi, L. (2018). Artifcial intelligence, deepfakes and a future of ectypes. *Philosophy & Technology*, 31, 317–321.
- Franks, A., & Waldman, A. E. (2019). Sex, lies, and videotapes: Deep fakes and free speech illusions. *Maryland Law Review*, 78(4), 892–898.
- Haemmerli, A. (1999). Whose who? The case for a Kantian right of publicity. *Duke Law Journal*, 49(2), 383–492.

- Harris, D. (2019). Deepfakes: False pornography is here and the law cannot protect you. *Duke Law & Technology Review*, 17, 99–127.
- MacKenzie, A., & Bhatt, I. (2020). Lies, bullshit and fake news: Some epistemological concerns. *Postdigital Science and Education*, 2, 9–13.
- Maras, M.-H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262.
- McKenna, M. P. (2005). The right of publicity and autonomous self-definition. *University of Pittsburgh Law Review*, 67, 225–294.
- Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.
- Öhman, C. (2020). Introducing the pervert's dilemma: A contribution to the critique of deepfake pornography. *Ethics and Information Technology*, 22, 133–140
- Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: Cyber subversion, information operations, and "deep fakes." *Australian Journal of International Affairs*, 74(4), 439–454
- Petty, R. D., & D'Rozario, D. (2009). The use of dead celebrities in advertising and marketing: Balancing interests in the right of publicity. *Journal of Advertising*, 38(4), 37–49.
- Phillips, W., & Wilner, R. M. (2017). The ambivalent internet: Mischief, oddity, and antagonism online. *Polity*.
- Polyakova, A. & Boyer, S. (2018). The future of political warfare: Russia, the West, and the coming age of global digital competition. *Brookings Institute*, March, 1–18.
- Post, R. C. & Rothman, J. E. (2020). The frst amendment and the right(s) of publicity. *Yale Law Review*, 130(1).
- Silbey, J.M., & Hartzog, W. (2019). The upside of deep fakes. *Maryland Law Review*, 78(4), 960–966.
- Spivak, R. (2019). 'Deepfakes': The newest way to commit one of the oldest crimes. *Georgetown Law Technology Review*, 3(2), 339–400.
- Stokes, P. (2012). Ghosts in the machine: Do the dead live on in Facebook? *Philosophy & Technology*, 25, 363–379.
- Swindell, J. S. (2007). Facial allograft transplantation, personal identity and subjectivity. *Journal of Medical Ethics*, 33(8), 449–453
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52.

- Wilson, D. G. (2017). The ethics of automated behavioral microtargeting. *AI Matters*, 3(3), 56–64
- Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B. & de Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, 14(1), 82–96

*****

A CRITICAL STUDY ABOUT COMBATING THE DARK SIDE OF AI: DEEPFAKE PREVENTION THROUGH ETHICAL AI DEVELOPMENT

Ankita Das[55] and Dr Manish Kumar Singh[56]

ABSTRACT

Deepfake technology has changed the way cybercrime is done and brought up important legal and ethical issues. This Article talks about how deep-fakes hurt weak groups, mainly by being used for bad things like spreading false information about politics, sharing sexual content without permission, and stealing identities. Artificial intelligence makes movies and pictures that look very real but are actually fake. Many people, especially women and famous people, lose money, their name, and their emotions because of deep-fakes. As deepfakes keep spreading, many are afraid that they could hurt trust in digital media and information that is open to the public. This Article is critical study of the ethical issues related to deep-fakes, with a focus on permission, privacy, and accountability. These problems with different countries' laws are brought to light because the current legal systems aren't thought to be strong enough to handle these issues. This Article looks at recent changes in the law and case studies from around the world to explore real-world answers to the issues raised by deepfakes. We need strong rules and standards that involve governments, IT companies, and regular people working together. At the end of the Research, it is suggested that people from different countries work together to combat the moral issues raised by deepfakes, while also encouraging digital responsibility and protecting those who are most at risk.

Keywords: Deep-fake technology, Cybercrime, Ethical challenges, Artificial intelligence (AI), Non-consensual pornography.

INTRODUCTION

Deepfake technology is maybe the most intriguing and concerning AI advancement. Deepfakes use AI algorithms, specifically generative adversarial networks, to create lifelike yet fake media. These technologies enable speech manipulation, visually engaging content that is practically indecipherable from actual media, and video face swapping. Deepfakes were first popular in gaming and entertainment, but their possible destructive applications have raised digital age worries.[57] Artificial intelligence and machine learning have made deepfakes popular. Since deepfake production tools become more available, they have been used in online communities and social media more and more. What started as a niche app has become a global phenomenon with major ramifications, especially in disinformation, identity theft, and unauthorised sharing. This article examines the social, legal, and ethical ramifications of deepfakes to promote accountability and prevention. This essay examines the dark side of deepfake technology and its threats to digital integrity, consent, and privacy. It will raise awareness of deepfake usage, show the need for tighter legislation, and show tech companies, social media platforms, and AI

[55] Research Scholar at NIMS school of Law (NIMS University Rajasthan), Jaipur, India.
[56] Assistant Professor at NIMS school of Law (NIMS University Rajasthan), Jaipur, India.
[57] Seng, L. K., Mamat, N., Abas, H., & Ali, W. N. H. W. (2024). AI Integrity Solutions for Deepfake Identification and Prevention. Open International Journal of Informatics, 12(1), 35-46.

developers' moral responsibilities to solve it. This essay will evaluate deepfakes' ethical issues and suggest answers and collaborations.

UNDERSTANDING DEEPFAKES: TECHNOLOGY AND APPLICATIONS

Artificial intelligence subfield generative adversarial networks (GANs) build deepfakes. GANs have opposing generator and discriminator neural networks. The generator creates fake images and videos, and the discriminator compares them to real data to determine realism. This confrontational method helps the generator develop hyper-realistic fake news with practice. These AI models employ large datasets like photographs or videos of a person to mimic their voice or appearance.[58] Despite their bad image, deepfakes have several legitimate uses. Entertainment filmmakers can de-age or recreate actors using deepfakes for visual effects. But deepfakes' dark side is troubling. One of the worst uses of deepfakes is to spread political disinformation by editing politician or other public figure videos. By superimposing women's faces over graphic material without their consent, non-consensual pornography causes considerable psychological and emotional suffering.

ETHICAL CHALLENGES OF DEEPFAKE TECHNOLOGY

Deepfake technology raises ethical concerns since it may violate consent and privacy. Non-consensual pornography in deepfake stands out. Sexually graphic images are often painted on people's faces without their consent, causing emotional, psychological, and social harm. Digital identity manipulation victims sometimes feel helpless since the legal system is unprepared to address such complicated situations. Deepfakes can impersonate people and threaten their privacy and security, in addition to non-consensual pornography.[59] Deepfake pornography disproportionately impacts women and other marginalised individuals and reinforces harmful stereotypes and intolerance. Movies and images are often manipulated to spread misinformation, harm reputations, and hurt leaders and celebrities. Deepfake creation tools are readily available, compounding these issues. Anyone with the right tools can spread dangerous information, mostly to conspicuous or weak targets.

Deepfakes exacerbate misinformation and online media distrust. Political disinformation campaigns are increasingly using deepfakes to sway public opinion. Many platforms can't moderate all content[60], and their procedures vary. Last but not least, those who create and propagate harmful deepfakes are culpable, but the internet and worldwide legal issues make it hard to hold them accountable. Lack of transparency increases the potential of deepfakes causing substantial damage.

LEGAL FRAMEWORKS: GLOBAL CHALLENGES AND GAPS

Deepfake technology is threatening legal systems worldwide. Deepfake laws are struggling to keep up with their rapid development. Some countries have been ahead of the curve in regulating deepfake

[58] Widder, D. G., Nafus, D., Dabbish, L., & Herbsleb, J. (2022, June). Limits and possibilities for "Ethical AI" in open source: A study of deepfakes. In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (pp. 2035-2046).

[59] Romero Moreno, F. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law, Computers & Technology, 1-30.

[60] Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. Journal of cyber policy, 5(2), 199-217.

usage, while others have lagged, leaving gaps that criminals can exploit.

Current Legal Frameworks

Certain countries have limited the harmful use of deepfakes in recent years. The EU's General Data Protection Regulation (GDPR) protects individuals' right to control their personal data, including likeness and photos. GDPR allows individuals to seek the removal of deepfakes that violate their privacy rights, and violators can be substantially fined. GDPR addresses privacy issues, although deepfakes are not directly addressed. Few US jurisdictions have passed laws against deepfake and other non-consensual pornography.[61] New laws in Texas and California make deepfakes for political campaigns and non-consensual pornography unlawful. AB 602 allows California victims of deepfake pornography to sue for damages. Deepfakes may also be susceptible to UK revenge pornography laws. Because there is no law addressing non-consensual deepfakes, victims have little options. South Korea, along with other Asian nations, has cracked down on cybersex crimes that use deepfake technology. These laws criminalise deepfake pornography production and distribution with serious penalties.

Legal Gaps

Despite progress, deepfake regulation worldwide is still lacking. Thus, victims are at risk in many countries without deepfake laws.[62] Since deepfake material can be generated in one country and shared worldwide, the internet's convoluted jurisdictional structure makes prosecution harder. Because deepfakes involve privacy, data protection, and intellectual property, present policies often fail to address them. Many countries still utilise outdated copyright, defamation, and fraud laws to combat deepfake usage. Internet anonymity makes deepfake prosecution harder. Even when dangerous content is identified, encrypted platforms or servers in locations with weak prohibitions make it difficult to trace its source. Deepfake victims must prove the content injured them. This is especially difficult with political influence and identity theft, where the harm is hard to measure but long-lasting.

Case Studies

Several major cases highlight the challenges court systems have in addressing deepfakes. In 2019, a deepfake video of the Belgian prime minister giving an insane climate change address went viral, causing great confusion until it was debunked. Despite no legal penalties, the film showed how deepfakes can disrupt politics. In another high-profile UK case, a woman's face was clearly featured on sexually graphic recordings. Despite her best efforts, she could not legally remove the recordings, and the perpetrator was never caught. This scenario showed why deepfake abuse laws are needed. A viral deepfake video misrepresented a political candidate in the 2020 Delhi elections in India, eliciting intense public anger. The country's outdated misinformation laws made it difficult to punish digital criminals, demonstrating the court system's inability to handle emerging crimes.

Cross-Border Complexities

[61] Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology innovation management review, 9(11).
[62] Labrecque, L. I., Peña, P. Y., Leonard, H., & Leger, R. (2024). Not all sunshine and rainbows: exploring the dark side of AI in interactive marketing. *Journal of Research in Interactive Marketing*.

Controlling deepfakes is difficult because the internet is available worldwide. You can make deepfake content in one country, post it to another, and see it elsewhere. In nations with weak or nonexistent deepfake legislation, offenders might exploit legal loopholes, making enforcement difficult owing to cross-border complexity. If a deepfake developer is based in a country without digital content modification laws, they are practically impossible to prosecute. Global collaboration is crucial, but cybercrime and intellectual property regimes often fail to address deepfake technologies.[63] Governments, tech companies, and international bodies must work together to regulate deepfakes. International treaties and regulations on deepfake technology exploitation should be adopted to handle these digital risks and overcome jurisdictional limitations. Deepfakes will exploit legal loopholes to prey on individuals and organisations till then.

ETHICAL AI DEVELOPMENT: PREVENTIVE MEASURES AGAINST DEEPFAKES

AI's rapid development of hyper-realistic deepfakes creates serious moral issues. Politicians, tech corporations, and AI experts must develop ethical methods to fight deepfakes. These challenges must be resolved to preserve individual rights, stop harmful content, and ethically develop AI.AI developers are crucial to fighting deepfake technology. Starting with ethics in AI system design is critical. In deepfake development and detection algorithms, developers must take measures. Deepfakes use GANs to simulate human behaviour. These algorithms must not be abused. AI should detect and report deepfake content to reduce dangers. Engineers should put ethics into AI systems from the start to prevent misuse. AI models' societal impact can be assessed using ethical auditing. Malicious deepfakes damage women and marginalised groups more than men. Software programmers can fix this by making datasets more representative of society and preventing AI systems from biassing data.

Role of IT Companies

IT, social media, and AI developers must stop deepfakes. Facebook, Twitter, and TikTok need tougher content monitoring since they distribute deepfake content. Tech firms may invest in deepfake detection. While many social media sites use AI-based algorithms to delete unwanted content, advanced technologies are needed to detect deepfakes before they spread virally. Platform users should check material.[64] Label altered or questionable media for viewer choice. Technology businesses should enforce community norms and punish deepfake content authors. Clear penalties like permanent bans or suspensions may deter repeat offenders. IT firms that boost privacy settings and give users more digital identity control limit deepfake manipulation.

AI and Human Rights

Human rights concerns surround AI-created deepfakes. Deepfake technology endangers dignity, autonomy, and security. Non-consensual pornography and political disinformation degrade people by

[63] Tremont, T. M. (2023). *Human-AI: Using Threat Intelligence to Expose Deepfakes and the Exploitation of Psychology* (Doctoral dissertation, Capitol Technology University).
[64] Fletcher, J. (2018). Deepfakes, artificial intelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal*, *70*(4), 455-471.

distorting their images. Other ethical issues exist beyond autonomy.[65] Fakes cause identity loss by making people say and do things they never did. Identity manipulation can have long-term implications on victims' personal and professional lives. Deepfake attacks on celebrities can alter public opinion and harm reputations. Deepfakes can also swindle, harass, and extort people, endangering their security. The complexity of AI-generated video makes deepfakes harder to spot, making them easier for bad actors to use. Legislators and AI developers must consider human rights while regulating deepfakes.

Emerging Technologies for Detection

Digital technologies to detect and stop deepfakes are needed as they get more complex. Because of this, AI-powered detection solutions have evolved. Deeptrace and Truepic are creating digital content change detection tools. Video and photo AI may detect unnatural face gestures, lighting, and audio-visual sync issues. Blockchain[66] and AI-based detection may assist verify digital content authenticity, which is growing more important. An immutable blockchain ledger preserves every file's origin and modification history, giving digital content makers confidence. The government may mandate media, law enforcement, and political campaigns use these technology to promote their adoption. Ethical AI research, proactive IT controls, and better detection tools are needed to mitigate AI-driven deepfakes. Ethical AI development and industry collaboration can stop deepfakes and restore digital media confidence.

THE ROLE OF SOCIAL MEDIA PLATFORMS

Social media helps spread and stop deepfakes. These platforms can prohibit deepfakes because they disseminate most digital material globally. To prevent deepfakes, platforms must manage content, reduce harm, and work with authorities and governments. Social media must moderate. Deepfakes transmit deceptive information, non-consensual pornography, and change users' identities. Social media, video sharing, and app firms are under pressure to stop them. Preventing deepfake content harm requires proactive content management. To stop its spread, promptly identify, mark, and remove modified media.

Digital material anomalies including distorted voice patterns, unusual lighting, and strange face motions can help automatic AI recognise deepfakes. AI alone won't work as deepfakes improve. Social networks need AI detection and human monitoring. By evaluating flagged content, skilled moderators can quickly eliminate dangerous content while keeping genuine submissions. Moderators must also be open. Platforms must explain how and why they delete deepfake content. Transparency about content removal and violation criteria creates trust and accountability. Social media platforms should allow users to report suspicious information to combat deepfakes.

Many social media companies tackled deepfake harm. Facebook prohibits election-influencing modified media. The company has enhanced real-time deepfake detection algorithms through academic cooperation and research. Facebook's 2020 "Deepfake Detection Challenge" trained AI to detect

[65] Qureshi, J., & Khan, S. (2024). Artificial Intelligence (AI) Deepfakes in Healthcare Systems: A Double-Edged Sword? Balancing Opportunities and Navigating Risks.
[66] Godulla, A., Hoffmann, C. P., & Seibert, D. (2021). Dealing with deepfakes–an interdisciplinary examination of the state of research and implications for communication studies. SCM Studies in Communication and Media, 10(1), 72-96.

deepfakes. Twitter now flags and removes misleading or harmful content. This includes scary or untrue deepfake videos.[67] Twitter tags help users evaluate content. YouTube, another big site, has also addressed deepfakes and political candidate falsehoods. Platforms will eliminate risky deepfake films. Films with non-consensual pornography, harassment, and fraud are included. Despite these efforts, many believe platforms should do more to stop deepfakes due to their prevalence.

Social media platforms realise they cannot fight deepfakes alone. Legal frameworks must be developed with governments for digital accountability and transparency. Governments may ban deepfakes on platforms. The GDPR prioritises privacy, but the DSA requires social media transparency and responsibility. Multinational task forces can share intelligence, confront new threats, and coordinate enforcement. Finally, social media must limit deepfake influence. Platforms can reduce deepfake content and make the internet safer by improving content control, harm mitigation, and government regulation. Companies may protect digital media ethics by being honest and proactive.

PROTECTING VULNERABLE GROUPS: GENDER-BASED VIOLENCE AND DISCRIMINATION

Women are being disproportionately targeted by non-consensual pornography and digital manipulation due to deepfake technology. Deepfake abuse victims, who are mostly women and marginalised people, often suffer psychological, social, and financial harm from having their faces on sexually explicit images and films without their consent. This exploitation reinforces a culture that regards women as objects by marginalising women and encouraging harmful gender norms. Race and LGBTQ+ people, who already face systemic prejudice, may be further victimised by deepfakes. People with bad motives are more likely to manipulate media to shame, blackmail, or degrade these communities. Deepfakes make it easy to create and disseminate fake news without penalties, worsening social inequality. Gender-based assault victims of deepfakes get legal and emotional support from multiple global groups. The UK has banned "revenge porn," which has helped prosecute deepfakes and other non-consensual pornography cases. Deepfake misuse might also trigger GDPR privacy laws.[68] However, these measures are still disconnected and require stronger, more comprehensive legislative frameworks and international collaboration to protect vulnerable groups. Governments, tech corporations, and advocacy groups must work together to improve detection, laws, and safe spaces for deepfake-related gender-based violence and prejudice victims.

TOWARDS DIGITAL RESPONSIBILITY: RECOMMENDATIONS FOR ETHICAL USE OF AI

We must fight deepfakes and establish AI ethics soon and collaboratively. Governments, tech corporations, and civil society must collaborate to pass legislation that promote ethical AI use and ban deepfakes. Deepfake technology abuse must be a cybercrime with sanctions by governments. To

[67] Battista, D. (2024). Political communication in the age of artificial intelligence: an overview of deepfakes and their implications. Society Register, 8(2), 7-24.
[68] Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media. Archives of Current Research International, 24(6), 355-375.

prevent dangerous deepfakes, AI engineers must integrate ethical checks. To stop the spread of altered material, governments and tech companies should create universal content moderation norms, which would require more internet platform monitoring. Public education and awareness are key to defeating deepfakes.[69] Digital literacy programmes should warn about deepfake technology and teach fake news detection and reporting. Teaching people to evaluate digital content's legitimacy can lessen deepfakes' social impact , deception and exploitation. For an informed and resilient populace, educational institutions, social media sites, and news organisations must participate in these initiatives.

Internet and deepfake threats are worldwide, requiring swift international coordination. Countries should form partnerships to address deepfake morality and exchange detection science. Hold criminals accountable International coalitions fighting cybercrime and data privacy could exploit jurisdictional loopholes. The combined effort would reduce global deepfake damage and boost digital responsibility.AI developments are needed for technology, but ethics must be balanced to minimise harm. AI research and development should be ethical to avoid societal injustice and human rights breaches. To guarantee AI developments are thoroughly examined before implementation, governments and tech corporations should create ethical regulatory agencies or advisory boards.[70] Tech companies can gain responsibility and confidence in their AI systems by revealing how their algorithms detect and handle deepfakes. Ethics allow us to investigate AI's potential without endangering society or human security. Finally, governments, industry leaders, and the public must handle deepfakes holistically. Implementing detailed policy frameworks, expanding digital literacy, boosting international collaboration, and preserving ethical AI development may balance technology innovation and social responsibility. Digital media integrity and online predator protection are key to fighting deepfakes beyond tech regulation.

CONCLUSION

In conclusion, this article has examined the ethical, legal, and societal implications of deepfake technology, highlighting the urgent need for robust regulatory frameworks and ethical AI development. We emphasized the disproportionate impact of deepfakes on vulnerable groups and the necessity for proactive measures from governments, tech companies, and civil society. A global response is essential to combat the challenges posed by deepfakes effectively. Looking ahead, fostering ethical AI development presents an opportunity to harness the positive potential of artificial intelligence as a force for good, promoting transparency, accountability, and digital responsibility in an increasingly complex digital landscape.

[69] Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. *Cyber defence in the age of AI, smart societies and augmented humanity*, 37-55.
[70] Wagner, T. L., & Blewer, A. (2019). "The word real is no longer real": Deepfakes, gender, and the challenges of ai-altered video. *Open Information Science*, *3*(1), 32-46.

NAVIGATING THE CYBER FRONTIER: LEGAL CHALLENGES AND RESPONSES TO CYBERCRIME IN INDIA

S. Indhu Dharshini[71] and Jeyasri S.[72]

ABSTRACT

Cybercrime has emerged as a significant threat in India affecting individuals, businesses and national security. With the rapid growth in digital technology and internet usage, there has been a surge in the number of cybercrimes such as hacking, identity theft, cyberbullying and data breaches. The legal framework for combating cybercrime in India revolves primarily around the Information Technology Act, 2000, which contains provisions to prevent and punish various cybercrimes. In addition, traditional laws such as the Indian Penal Code are also applicable to cybercrimes, including offences such as fraud, defamation and forgery. To stop and punish cyber criminals, "cyber laws" have been introduced. Cyber laws can be defined as the law of the Internet. It is the part of the legal system that deals with the Internet, cyberspace and other legal issues such as online security and online privacy. Studying this can help researchers, policymakers, legal professionals, and law enforcement agencies take proactive steps to combat this growing threat, protect individuals and organizations, and ensure a safe digital environment. The study aims to contribute to the enhancement of the legal framework, providing a data-driven approach to improving victim support and protection in the digital space.

Keywords: Cybercrime, digital space, victim challenges, legal framework, demographic factors, preventive reforms, cybercrime awareness.

BACKGROUND

The rise of the internet and the widespread use of digital technology have radically altered the way people interact, communicate, and do business as a result of the growing usage of digital technology and the internet. Although there are many advantages to these developments, they have also led to the emergence of cybercrime, a new category of criminal conduct. Cybercrime pertains to illicit actions that are enabled or carried out using computers, networks, and the Internet.

Cybercriminals use flaws in computer networks, systems, and online platforms to commit a range of criminal activities. Phishing, impersonation, identity theft, cyberbullying, child pornography, and domain name conflicts are a few of them. Cybercrime may have detrimental effects on people's finances, relationships, and mental health. These effects extend beyond individuals to include governments, businesses, and even national security. Policymakers and legal professionals may create strong legal frameworks to successfully tackle cybercrime by analysing these problems.

In the future, as cyber threats grow more sophisticated with advancements like AI and quantum computing, legal frameworks will need to adapt rapidly to address new challenges. Stronger international cooperation, real-time digital forensics, and evolving privacy laws will be crucial in ensuring a safer digital environment.

[71] Student at Sastra Deemed To Be University, Thanjavur, Tamil Nadu, India.
[72] Student at Sastra Deemed To Be University, Thanjavur, Tamil Nadu, India.

LITERATURE REVIEW

Cybercrime Trends and Patterns - This review examines various trends and patterns in cybercrime, focusing on types of cyber offenses, perpetrator behaviors, and technological advancements. It provides a comprehensive overview of cybercrime statistics. Legal Frameworks for Cybercrime Prevention - This literature review explores existing legal frameworks and policies designed to combat cybercrime. It analyzes how laws are implemented and their effectiveness in deterring cybercriminals. Technological Solutions to Cybercrime - This review focuses on technological solutions and advancements aimed at preventing cybercrime. It emphasizes software and hardware developments without considering how these measures impact victims or the necessity of victim feedback in creating effective technologies. Cybercrime and Social Media: A Review of Threats - This literature review addresses various threats associated with cybercrime in the realm of social media, such as phishing, hacking, and identity theft.

Perpetrator Motivations in Cybercrime - This review investigates the motivations behind cybercriminal behaviours, exploring factors such as financial gain, ideological beliefs, and psychological profiles. It offers valuable insights into why crimes occur. Cybersecurity Measures: Efficacy and Challenges - This literature review analyses various cybersecurity measures and their effectiveness in preventing cybercrime. It discusses institutional and organizational approaches. The Role of Law Enforcement in Cybercrime Investigation - This review explores the role of law enforcement agencies in investigating and prosecuting cybercrime. It focuses on procedural aspects and challenges faced by law enforcement.

RESEARCH PROBLEM

To analyse the challenges faced by victims, providing a more comprehensive view of legal issues in India from their perspective.

RESEARCH OBJECTIVES

1. To examine different types of cybercrime to gain a comprehensive understanding of the range of criminal activities carried out in the digital space.
2. To find out the awareness of internet users about cybercrime.
3. To propose preventive reforms and effective regulations to control cybercrime.

RESEARCH QUESTION

Whether demographic factors, such as age and gender, influence individuals' experiences with cybercrime, including their likelihood of reporting such incidents?

RESEARCH HYPOTHESIS

Demographic factors such as age and gender significantly influence individuals' experiences with cybercrime, impacting the likelihood of encountering cybercrime and reporting incidents.

RESEARCH METHODOLOGY

The Research Design is Empirical Research, Sample was the Population Aged between 20 to 50 irrespective of their gender & ethnicity.

The objectives of the study were to study the level of awareness amongst people, and to study the measures taken by people to prevent cybercrime.

The sample size consists of 122 general public opinions both males and females and the Sampling Method was Stratified Technique for this research. The data was collected from people all across India with the help of the Tools that is Google Forms, Questionnaire of 20 questions.

UNDERSTANDING THE CYBER CRIMES

Cybercrime refers to criminal activities carried out using digital technology, computer networks or the Internet. It involves the unauthorised use of information and communication technology to carry out illegal activities, exploit vulnerabilities or cause harm to individuals, organisations or society as a whole. Preventing and combating cybercrime requires strong cybersecurity measures, effective legislation and advances in technology and digital forensics.

It threatens an individual's privacy by disclosing or publishing their personal or confidential information online with the intention of damaging their reputation and causing physical or mental harm, directly or indirectly.

CATEGORIES OF CYBERCRIME

Cybercrime is not limited to a few types known to Internet users but they are constantly evolving with new strategies, posing challenges to stop them.

1. Crimes against individuals

Crimes that harm specific individuals. These crimes include harassment by email, online harassment, cyberbullying, dissemination of obscene material, defamation, copyright infringement, hacking, electronic message address theft, SMS theft, wiretapping, fraud and deception, child pornography, intimidation, denial of service, spoofing and fraud.

A) Cyber stalking

It means to create a physical threat that creates fear using computer technology such as the internet, e-mail, phones, text messages, webcam, websites or video.

B) Hacking:

It means unauthorised control/access over a computer system and an act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hack telecommunication and mobile networks.

C) Child Pornography:

It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

D) Assault by Threat:

refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

E) Cheating & Fraud:

It means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with a guilty mind which leads to fraud and cheating.

2. Crimes against Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents.

A) Cyber Squatting:

It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

B) Intellectual Property Crimes:

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

C) Cyber Vandalism:

Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

D) Transmitting Virus:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

E) Cyber Trespass:

It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

F) Identity theft

It is a form of fraud or simply deceit that is done by using the personal information of someone else whose information is not authorised to be used by someone other than him under the law. Section 66C of the Information Technology Act, 2000 provides for punishment for identity theft. It says if anyone fraudulently or dishonestly uses any electronic signature, password, or unique identification feature of

any other person, they are guilty of identity theft and liable for imprisonment of either description for a maximum of three years and a fine up to one lakh rupees.

3. Cybercrimes against Government

A) Possession of Unauthorized Information:

It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

B) Cyberterrorism:

Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

C) Distribution of pirated software:

It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

NEED FOR CYBERCRIME LAWS IN INDIA

- Cyberlaw is of particular importance in countries such as India, where the internet is used widely. In order to protect both individuals and organizations against cyber crime, the law was enacted. The cyberlaw allows other people or organizations to take legal action against someone if that person violates and breaks the provisions of the law.
- Cyberlaw may be required in the following circumstances:
- Due to the fact that all the transactions associated with stocks are now executed in demat format, anyone who is involved with these transactions is protected by cyber law in the event of any fraudulent transactions.
- Almost all Indian companies have electronic records. A company may need this law to prevent the misuse of such data.
- As a result of the rapid development of technology, various government forms are being filled out electronically, such as income tax returns and service tax returns. Anybody can misuse those forms by hacking government portal sites, and thus, cyberlaw is required under which legal action can be taken.

WHO ARE VICTIMS OF CYBERCRIME IN INDIA?

Defining victims of cybercrime in India presents challenges similar to those encountered in defining cybercrime itself. To understand the concept of a cybercrime victim in the Indian context, we can refer to guidelines such as the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985). According to this declaration, victims are individuals or groups who have

suffered harm—be it physical, mental, emotional, or economic—or experienced a significant violation of their fundamental rights due to acts or omissions that contravene criminal laws.

Two key aspects emerge from this definition within the Indian context. Firstly, the classification of a victim relies heavily on the nature of harm suffered. Victims can be seen as those affected both materially and non-materially by cybercrime. Secondly, victims can be categorized into two groups: direct victims—those who suffer directly from the cybercrime—and indirect victims, including family members or dependents of the direct victim. Although the primary focus is typically on direct victims, the definition may also encompass immediate relatives in relevant circumstances, particularly in cases involving emotional or psychological harm.

A significant case that illustrates the impact of cybercrime on victims in India is the Avinish Bajaj school porn case (2008). In this incident, a minor student was subjected to severe harassment after an intimate video was circulated online without consent. The case highlighted the devastating emotional and psychological toll on the victim, demonstrating the need for robust protections against such violations. The Supreme Court's decision underscored the importance of addressing the rights of victims in cases involving non-consensual content, emphasizing that victims should be treated with sensitivity and afforded legal recourse.

This case exemplifies the necessity of acknowledging and addressing the complexities surrounding victims of cybercrime in India, ensuring that both direct and indirect victims receive the support and justice they deserve.

A. Physical Impacts:

In addition to damaging assets like computer hardware or infrastructure, certain cybercrimes can lead to severe consequences for individuals, including physical harm and even loss of life. Cyberbullying, cyberstalking, and other forms of online harassment have been linked to serious psychological distress, which, in extreme cases, can lead to self-harm or suicide. Victims of cyberbullying, particularly vulnerable individuals such as teenagers or those already facing mental health challenges, may experience overwhelming feelings of isolation, depression, or helplessness, sometimes culminating in tragic outcomes like suicide.

These cyber-attacks not only affect mental health but can also push victims towards physical harm. For example, non-consensual dissemination of intimate images, often referred to as "revenge porn," can leave victims feeling violated and lead to severe psychological trauma, resulting in physical harm or even death in some cases.

Beyond the individual level, damage to physical infrastructure from cybercrimes, such as attacks on hospitals or emergency services, can disrupt essential services, potentially putting lives at risk. These cascading effects can impact not only victims directly targeted by cybercriminals but also broader segments of society, heightening the need for robust cybersecurity measures and support systems for victims.

B. Financial Impacts:

Cybercrime can cause substantial financial damage to both businesses and individuals. Even a single cyberattack can lead to significant financial losses. For instance, the 2017 WannaCry ransomware attack affected around 230,000 computers globally, resulting in an estimated financial loss of US$4 billion. Additionally, the global cost of cybercrime is estimated to reach $1 trillion annually, though these figures often reflect broader national economic impacts rather than the specific financial burden on individual victims.

In India, cybercrimes have also had serious financial repercussions. For example, the 2018 Cosmos Bank cyberattack resulted in a loss of nearly INR 94 crores after hackers infiltrated the bank's server and siphoned funds via fraudulent ATM transactions. Similarly, the Punjab National Bank scam, one of the largest frauds in Indian banking history, involved the misuse of the SWIFT system to illegally transfer INR 11,400 crores.

On a personal level, individuals in India are frequently targeted by phishing scams, identity theft, and online financial fraud, leading to significant monetary loss. These attacks often target vulnerable populations who may not have access to cybersecurity education, further exacerbating the financial burden on victims. As cybercriminals employ increasingly sophisticated methods, the financial toll on Indian businesses and individuals continues to rise, demanding stronger cybersecurity measures and legal frameworks to address the issue.

C. Psychological and Emotional Impacts:

Cybercrime can have profound psychological and emotional effects on individuals. Victims may experience a range of emotions, including anger, anxiety, fear, and a loss of confidence in technology. They often feel ashamed, vulnerable, or powerless, which can lead to depression. This is particularly true for victims of online abuse, such as cyberstalking, doxing, harassment, or the non-consensual dissemination of intimate images. Many victims internalize guilt and self-blame, compounding their psychological distress.

In India, several case laws highlight the emotional toll of cybercrime on victims. For instance, the landmark case of Shreya Singhal v. Union of India (2015) addressed the issue of Section 66A of the Information Technology Act, which was used to penalize offensive online messages. The Supreme Court ruled the provision unconstitutional, emphasizing the need to protect individuals from arbitrary online harassment while also recognizing the psychological impact that cyberbullying and online threats can have on victims.

Another relevant case is *Sakshi v. Union of India* (2004), where the Supreme Court recognized the need to protect minors from sexual abuse in the digital space, leading to more stringent laws against online harassment and exploitation. This case brought attention to the emotional trauma experienced by victims of such crimes, emphasizing the importance of providing psychological support and legal recourse.

Furthermore, in the case of Sushmita v. State of Maharashtra (2018), the victim of non-consensual sharing of intimate images sought justice, highlighting the severe emotional distress caused by the act.

The court's recognition of the victim's suffering underscored the need for comprehensive measures to address the psychological impact of cybercrimes.

These cases illustrate not only the legal framework surrounding cybercrime in India but also the importance of acknowledging and addressing the psychological and emotional impacts on victims, which can have lasting effects on their mental health and well-being.

D. Reputational Impacts:

In addition to financial losses, cybercrime can significantly harm reputations. At the organizational level, a cyber incident can tarnish a company's image, erode customer trust, damage public perception, and reduce business opportunities. For individuals, the exposure of private information during a cyberattack can severely damage their reputation, especially if the leaked information is sensitive or damaging.

In India, several high-profile cases illustrate the reputational impacts of cybercrime. For example, the 2018 data breach at the online food delivery service Zomato exposed the personal data of over 17 million users, including email addresses and hashed passwords.

This incident not only resulted in financial losses for the company but also raised concerns among customers regarding data security, leading to a decline in user trust and potentially impacting business opportunities.

Another notable case is the data breach involving the hotel chain Marriott International, which affected over 5 million Indian guests. The exposure of sensitive personal information raised serious questions about the company's cybersecurity measures and resulted in significant reputational damage, as customers began to doubt their data's safety with the brand.

On an individual level, incidents of doxing—where personal information is publicly disclosed without consent—can lead to severe reputational harm. For instance, the case of a prominent Indian actress whose private images were leaked online led to widespread media coverage and public scrutiny, impacting her personal and professional life.

This incident not only highlighted the severe emotional distress faced by the victim but also underscored the broader societal implications of reputational damage resulting from cybercrime. These examples demonstrate that the reputational impacts of cybercrime can be profound, affecting both organizations and individuals in India. The erosion of trust, damage to public perception, and the potential for lost business opportunities highlight the need for robust cybersecurity measures and proactive responses to incidents.

WHAT ARE THE NEEDS OF VICTIMS OF CYBERCRIME?

By all accounts, victims' needs can be diverse, as the impacts of cybercrime on them can range from material, such as financial loss, to non-material, including reputational damage and psychological and emotional distress. Some victims may have suffered financial loss and require compensation. When victims continue to experience the negative consequences of cybercrime, they may adopt a more punitive stance and seek to prosecute the offender. However, for others, there can be more pressing

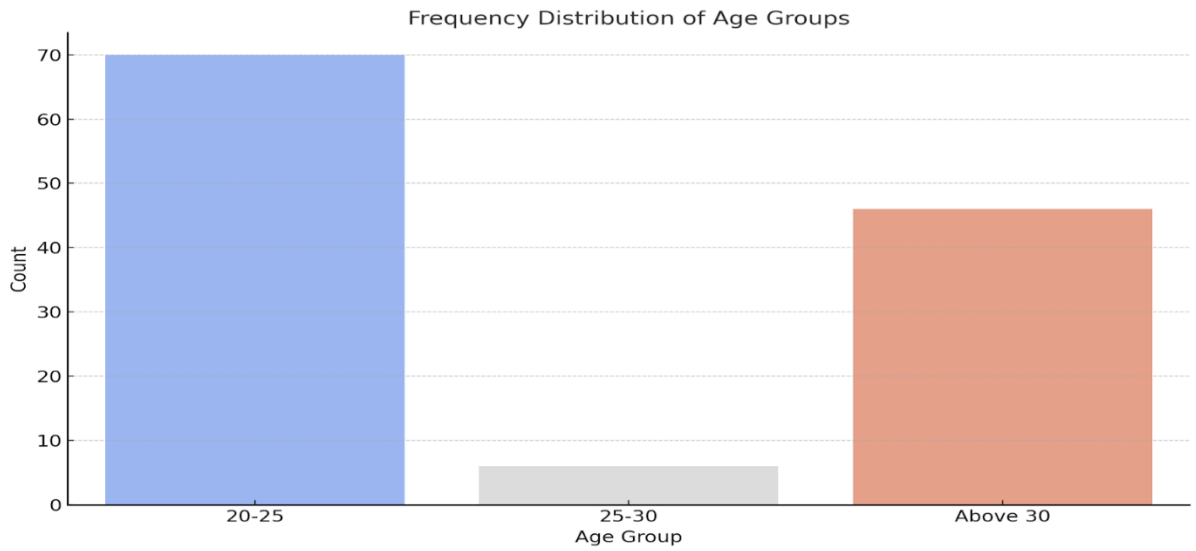
matters than retribution. These needs may include an apology, assistance and protection, recognition and condemnation of the harm, guarantees of safety, restoration to the situation preceding the cyber incident, prevention of the recurrence of the cybercrime, or participation in criminal proceedings.

In India, the needs of victims can also include immediate responses, such as the removal of illegal content posted online. For instance, in cases of cyberbullying or the non-consensual sharing of intimate images, victims may require urgent action to mitigate further harm and restore their dignity. Additionally, some victims may require responses that take into account their specific vulnerabilities and needs, such as psychological support or counseling services.

It is important to acknowledge that victimhood varies depending on various factors, including individual vulnerabilities, psychological perspectives, and age-related differences.

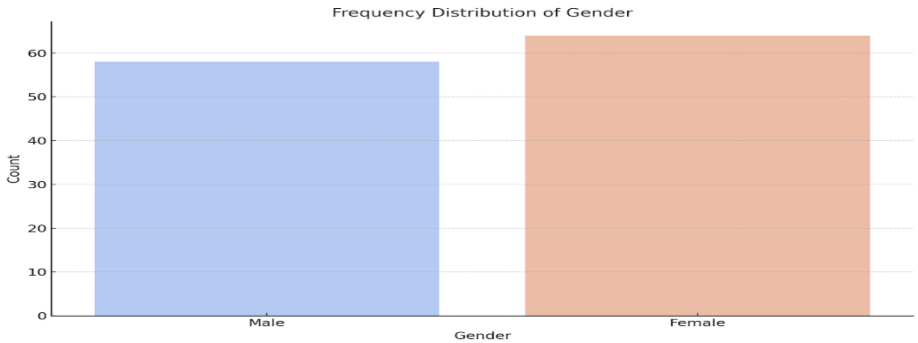
VISUALISATION OF DATA

1. **Age**



- The bar chart below represents the distribution of respondents across different age groups.
- The majority of the respondents (57%) fall within the **20-25 age group**. The next largest group is **Above 30** (38%), followed by a small portion of respondents aged **25-30** (5%).

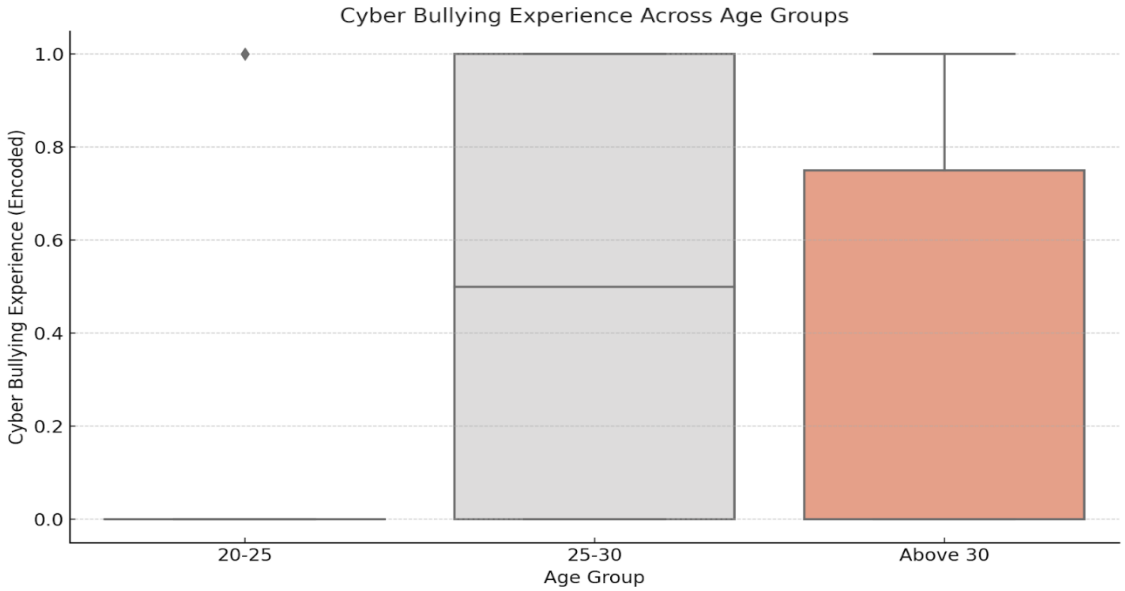
2. **Gender**



- The respondents are nearly evenly split between genders, with **52% female** and **48% male**.

Gender	No Cyberbullying	Yes Cyberbullying
Male	53	11
Female	43	15

3. **Cyber Bullying Experience Across Age Groups**

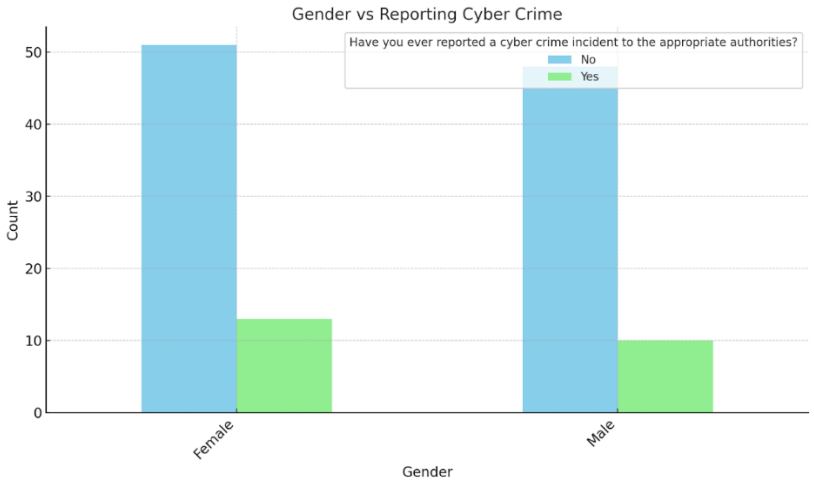


- About **21% of respondents** have experienced cyber bullying (mean value of 0.21 for the encoded data).
- The cross-tabulation analysis shows that individuals in the **20-25 age group** have reported the highest number of cyber bullying incidents. Out of the 70 respondents in this age group, 11 (16%) have experienced cyber bullying. In contrast, individuals **Above 30** report cyber bullying at a slightly higher rate (26%) compared to the other groups.

Age Group	No Cyber bullying	Yes Cyber bullying
20-25	59	11
25-30	3	3
Above 30	34	12

- Younger individuals (20-25) report more cyber bullying incidents in total, but the relative percentage is higher among respondents above 30.

4. **Gender & Reporting Cyber Crime**



- About **19% of respondents** have reported cybercrimes to authorities
- The cross-tabulation indicates that **males** are slightly more likely to report cyber bullying than females. **15 males** (26%) reported experiencing cyber bullying, compared to **11 females** (17%).

Gender	No Report	Yes Report
Male	48	10
Female	51	13

- The analysis shows that **females** are slightly more likely to report cybercrimes than males. **13 females** (20%) reported cybercrimes, compared to **10 males** (17%).

5. **Age & Reporting Cyber Crime**

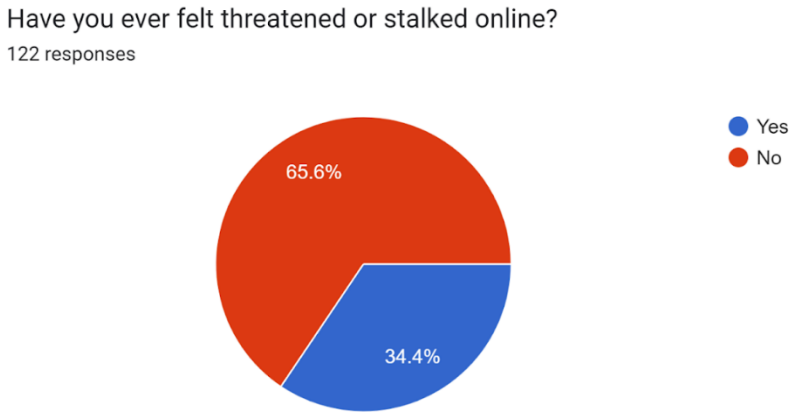
- This cross-tabulation helps us understand how the tendency to report cyber crimes varies by age group.

- The cross-tabulation reveals that **20-25 year-olds** are the most likely to report cyber crimes, with **14 individuals** (20%) having reported incidents. Individuals **Above 30** have a lower reporting rate (15%).

Age group	No Report	Yes Report
20-25	56	14
25-30	04	02
Above 30	39	07

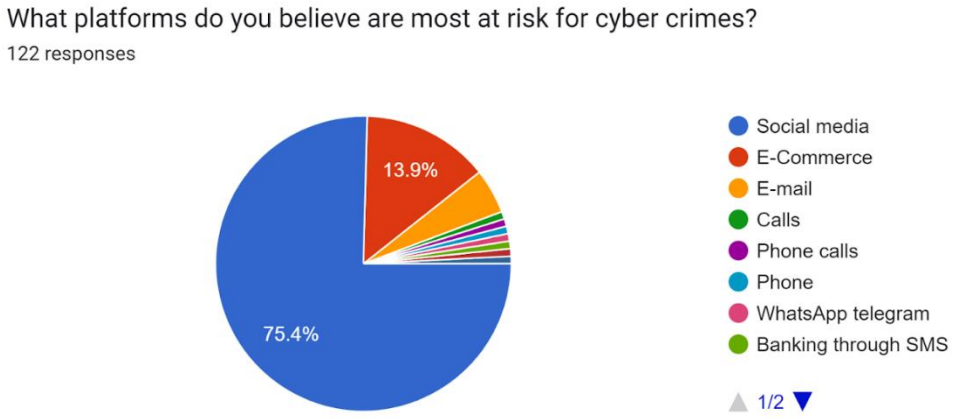
- Younger individuals are more likely to report cyber crimes, possibly due to greater awareness or confidence in the reporting process.

6. **Have you ever felt threatened or stalked online?**



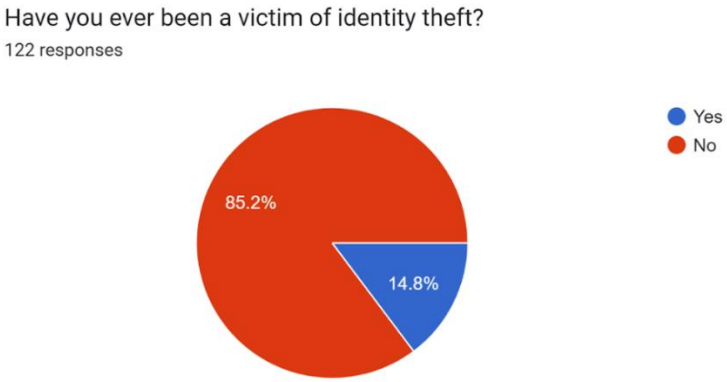
- 65.6% of respondents have never felt threatened or stalked online.
- 34.4% of respondents have felt threatened or stalked online.

7. **What platforms do you believe are most at risk for cyber crimes?**



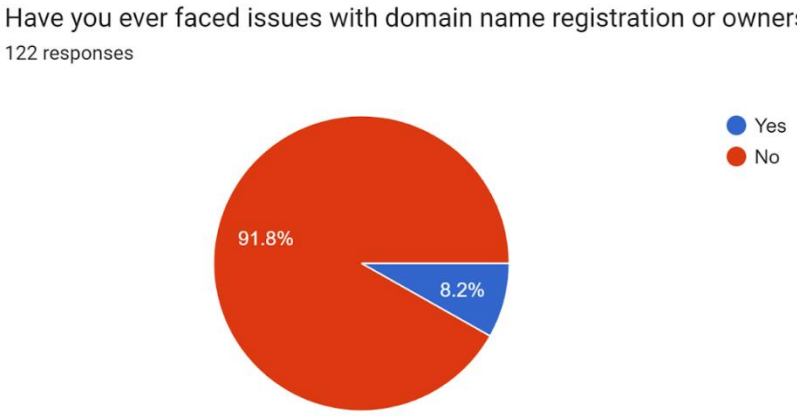
- 75.4% of respondents believe that social media platforms pose more risk for cyber crimes.

8. **Have you ever been a victim of identity theft?**



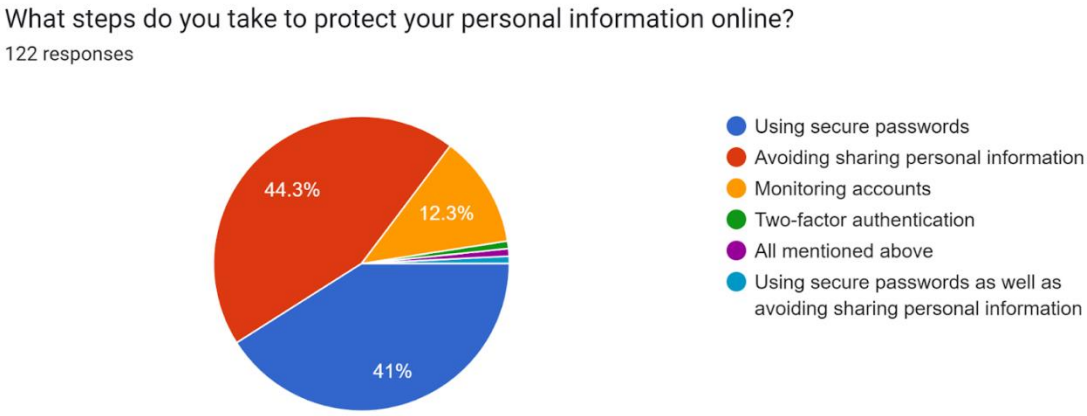
- 85.2% of respondents have never been a victim of identity theft.
- 14.8% have been a victim of identity theft.

9. **Have you ever faced issues with domain name registration or ownership?**



- 91.8% have never faced issues with domain registration or ownership.
- 8.2% have faced issues with domain registration or ownership.

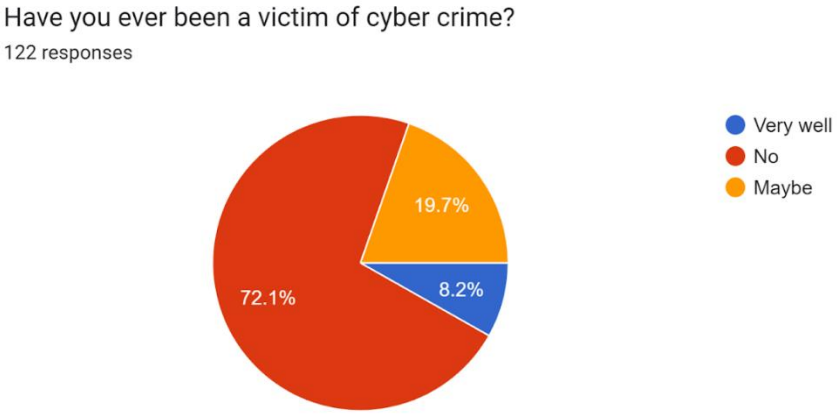
10. **What steps do you take to protect your personal information online?**



- 44.3% of respondents believe avoiding sharing personal information can protect their personal information online.
- 41% of respondents believe using secure passwords can protect their personal information online.

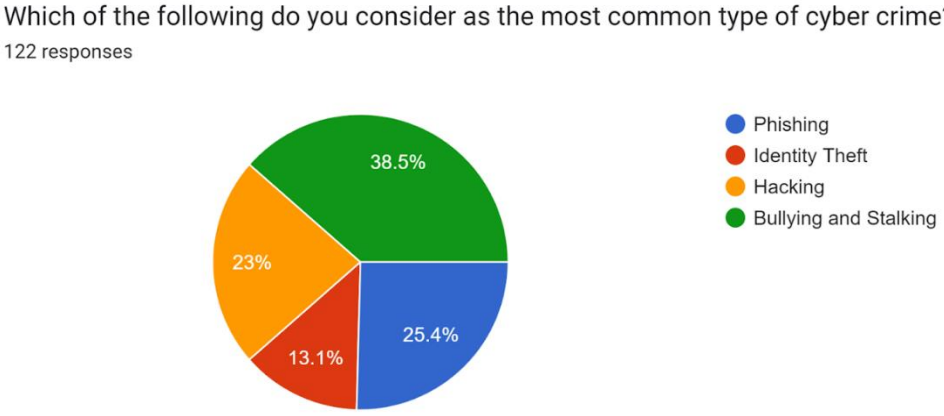
- 12.3% of respondents believe monitoring accounts can protect their personal information online.

11. **Have you ever been a victim of cyber crime?**



- 72.1% of respondents have not been a victim of cyber crime.
- 19.7% of respondents are not sure about it.
- 8.2% of respondents have been a victim of cyber crime.

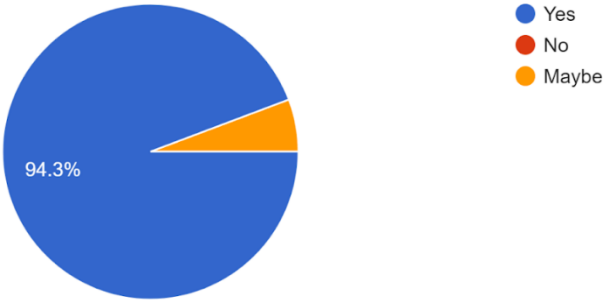
12. **Which of the following do you consider as the most common type of cyber crime?**



- 38.5% of respondents consider bullying and stalking as the most common type of cyber crime.
- 25.4% of respondents consider phising as the most common type of cyber crime.
- 23% of respondents consider hacking as the most common type of cyber crime.
- 13.1% respondents consider identity theft as the most common type of cyber crime.

13. **Do you believe cyber crime is increasing in today's digital world?**

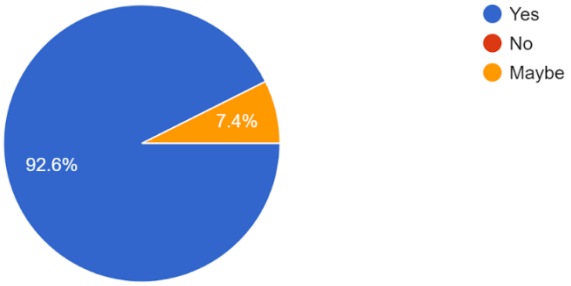
Do you believe cyber crime is increasing in today's digital world?
122 responses



- 94.3% of respondents believe cyber crime is increasing in today's digital world.

14. **Do you believe individuals should take more responsibility for protecting themselves from cyber crime?**

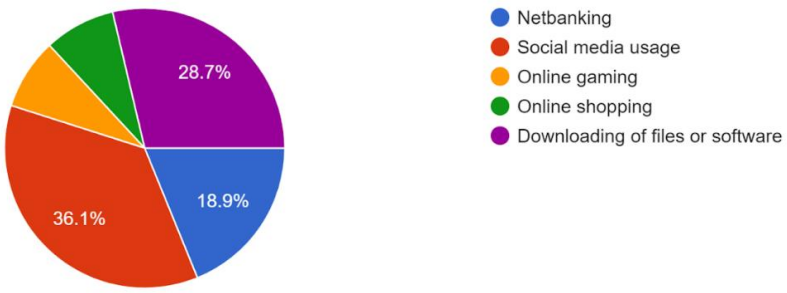
Do you believe individuals should take more responsibility for protecting themselves from cyber crime?
122 responses



- 92.6% of respondents believe individuals should take more responsibility for protecting themselves from cyber crime.
- 7.4% of respondents are not sure about individuals should take more responsibility for protecting themselves from cyber crime.

15. **Which of the following online activities do you consider the most vulnerable to cyber crime?**

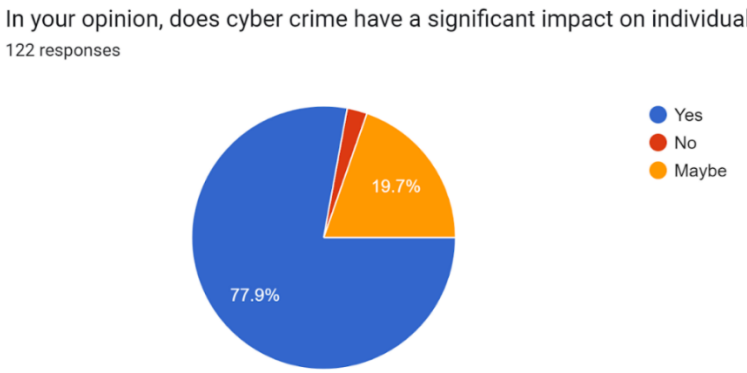
Which of the following online activities do you consider the most vulnerable to cyber crime?
122 responses



- 36.1% of respondents consider social media usage is the most vulnerable to cyber crime.

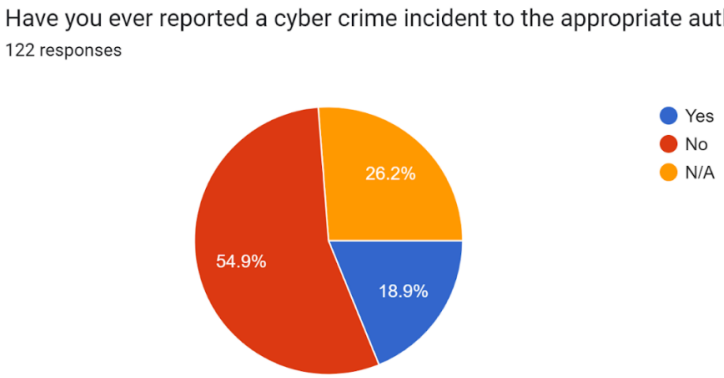
- 28.7% of respondents consider downloading files or software is the most vulnerable to cyber crime.
- 18.9% of respondents consider netbanking is the most vulnerable to cyber crime.

16. **In your opinion, does cyber crime have a significant impact on individuals' daily lives?**



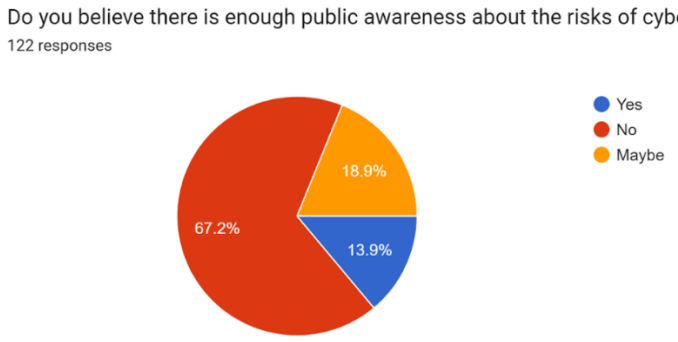
- 77.9% of respondents believe cyber crime has a significant impact on individual's daily lives.
- 19.7% of respondents are not sure about it.

17. **Have you ever reported a cyber crime incident to the appropriate authorities?**



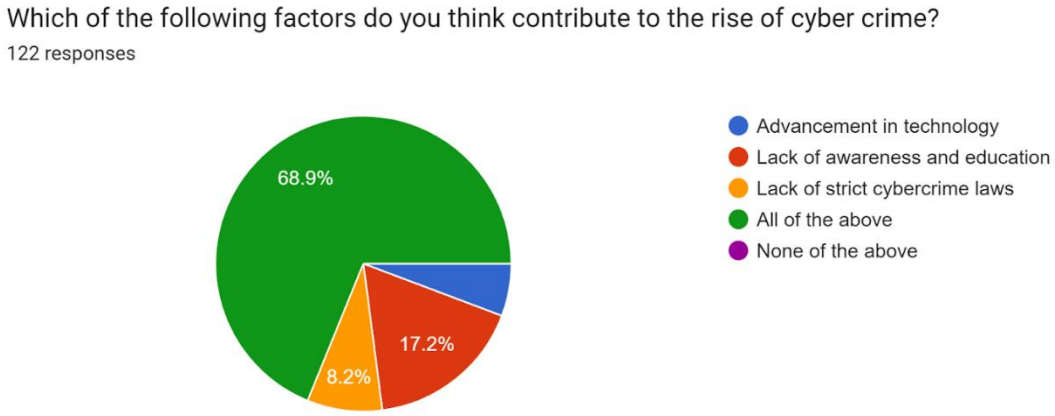
- 54.9% of respondents have never reported a cyber crime incident to the appropriate authority.
- 26.2% of respondents are not sure about it.
- 18.9% of respondents have reported a cyber crime incident to the appropriate authority.

18. **Do you believe there is enough public awareness about the risks of cyber crime?**



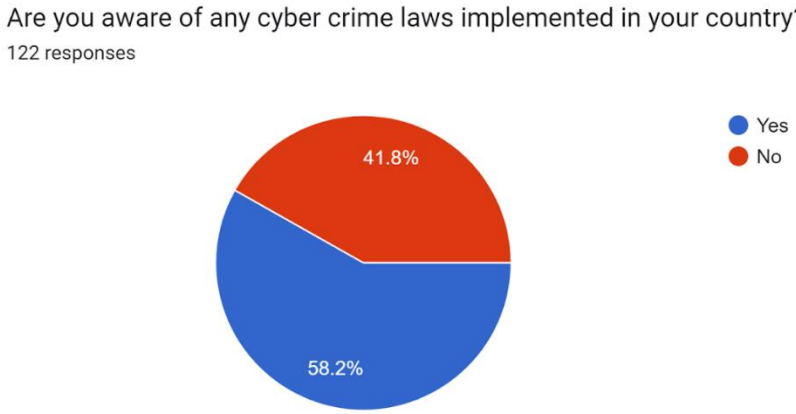
- 67.2% of respondents believe that there is no enough public awareness about the risks of cyber crime.
- 18.9% of respondents are not sure about it.
- 13.9 % of respondnets believe that there is enough public awareness about the risk of cyber crime.

19. **Which of the following factors do you think contribute to the rise of cyber crime?**



- 68.9% of respondents believe all the factors contribute to the rise of cyber crime.

20. **Are you aware of any cyber crime laws implemented in your country?**



- 58.2% of respondents are aware of cyber crime laws implemented in their country.
- 41.8% of respondents are not aware of cyber crime laws implemented in their country.

CONCLUSION OF THE ANALYSIS

- The objective of this analysis was to explore relationships between demographic factors (age and gender) and experiences with cybercrime, including cyber bullying and the reporting of cyber crime incidents.
- The majority of respondents were between the ages of 20-25 (57%) and the gender distribution was nearly even, with 52% female and 48% male. About 21% of respondents reported experiencing cyber bullying, while only 19% reported having reported cyber crime incidents.

- Younger individuals (20-25) reported the most cyber bullying incidents in absolute numbers, but individuals above 30 showed a higher relative rate of experiencing cyber bullying. Males reported slightly more cyber bullying incidents than females. Reporting of cyber crime was generally low, with younger individuals (20-25) slightly more likely to report incidents.

SCOPE AND LIMITATIONS

Scope:

1. Focus on Victim-Centric Approach: This research aims to provide insights into the experiences of cybercrime victims in India, emphasizing their perspectives on legal issues and the challenges they face. By exploring demographic factors such as age and gender, the study seeks to understand how these variables affect individuals' encounters with cybercrime.
2. Broad Range of Cybercrime Types: The research encompasses various forms of cybercrime, including but not limited to cyberbullying, identity theft, phishing, and online harassment. This wide lens allows for a comprehensive understanding of the impact of cybercrime on different demographic groups.
3. Quantitative Analysis: Utilizing quantitative methods, including surveys and statistical analysis, the study aims to establish relationships between demographic factors and experiences with cybercrime. This will provide empirical evidence to support or refute the research hypothesis.
4. Implications for Policy and Legal Reform: The findings will offer recommendations for improving legal frameworks and victim support services in India, thereby contributing to the development of more effective policies and interventions aimed at safeguarding potential victims of cybercrime.

Limitations:

1. Sample Size and Diversity: The research may be limited by the size and diversity of the sample population. A smaller or non-representative sample could affect the generalizability of the findings to the wider population.
2. Self-Reported Data: The reliance on self-reported data from surveys may introduce bias, as individuals may underreport or overreport their experiences with cybercrime due to fear of stigma or a lack of awareness about certain incidents.
3. Focus on Demographic Factors: While the study concentrates on age and gender, other relevant factors such as socioeconomic status, education level, and geographic location might also influence experiences with cybercrime but may not be adequately addressed.
4. Dynamic Nature of Cybercrime: The constantly evolving landscape of cybercrime may limit the relevance of the findings over time. New forms of cybercrime and changing victim experiences may necessitate ongoing research beyond the scope of this study.

5. Cultural Context: The study's findings may be influenced by the cultural context of India, which may not be applicable to other regions or countries with different social norms and legal frameworks regarding cybercrime.

RECOMMENDATIONS

(A) Upgraded Casualty Bolster Services:

Establish devoted bolster frameworks for cybercrime casualties that incorporate mental counselling, lawful help, and emergency intercession administrations. These assets ought to be effectively available and custom-made to address the particular needs of diverse casualty bunches, counting minors and marginalized communities.

(B) Public Mindfulness Campaigns:

Implement comprehensive open mindfulness campaigns to teach people around the dangers of cybercrime and the accessible assets for casualties. These campaigns ought to center on preventive measures, announcing components, and the significance of cybersecurity practices.

(C) Strengthening Announcing Mechanisms:

Develop streamlined and secret detailing instruments for casualties of cybercrime. This seem incorporate a centralized online stage where casualties can report occurrences, look for help, and track the advance of their cases. Guaranteeing secrecy and assurance for casualties amid the announcing prepare is crucial.

(D) Victim-Centric Preparing for Law Enforcement:

Provide specialized preparing for law requirement organizations on taking care of cybercrime cases with a center on the needs and rights of casualties. Preparing ought to incorporate affectability preparing, understanding the mental impacts of cybercrime, and successful communication strategies.

(E) Legal System Enhancements:

Advocate for the consolidation of casualty rights inside existing legitimate systems related to cybercrime. This incorporates guaranteeing that casualties have the right to take part in lawful procedures, get opportune overhauls almost their cases, and get to compensation for harms incurred.

(F) Research on Casualty Experiences:

Conduct in-depth investigate thinks about to investigate the encounters of cybercrime casualties in India. Gathering subjective information on their challenges, needs, and results can offer assistance educate arrangements and hones that superior bolster casualties in the repercussions of cyber incidents.

(G) Collaboration with NGOs and Community Organizations:

Foster associations with non-governmental organizations and community bunches that specialize in casualty back and promotion. Collaborating with these organizations can upgrade outreach endeavors and guarantee that casualties get all encompassing support.

(H) Focus on Recovery and Reintegration:

Develop recovery programs that help casualties in revamping their lives after cybercrime episodes. This seem incorporate professional preparing, counseling, and community engagement activities pointed at lessening disgrace and advancing reintegration.

(I) Promoting Cyber Cleanliness Education:

Integrate cyber cleanliness instruction into school curriculums to engage youthful individuals with information around online security, computerized impressions, and mindful web utilize. This proactive approach can offer assistance decrease the number of future victims.

(J) Monitoring and Evaluation:

Establish instruments for continuous observing and assessment of casualty back administrations and approaches related to cybercrime. Standard evaluations can offer assistance distinguish holes, degree viability, and illuminate future enhancements in victim-centric approaches.

CONCLUSION

Cybercrime is one of the most significant problems for countries around the world today. This includes unauthorised access to information and violates security such as privacy, passwords, etc. Anyone who has Internet use. Cyber theft is a part of the cybercrime, which means robbery performed via computer or the Internet. With an increase in the number of cyber security fraud and crimes, the government is developing advanced rules that will safeguard the interests of people and protect people from any negative events happening online.

*****

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER CRIME

Mandeep Sharma[73] and Nitu[74]

ABSTRACT

Artificial Intelligence (AI) is a popular term in the cyber world. It is still an emerging science in many areas in response to the problems of the twenty-first century. Artificial intelligence is now inextricably linked to human existence. Today, it is impossible to envision a future without AI since technology has such a profound influence on human existence. The primary goal of AI is to construct technology-based activities that represent human knowledge in order to solve issues. Simply put, AI is the study of how people think, work, learn, and make decisions in all aspects of life, whether it's problem solving, learning new things, thinking rationally, arriving at a solution, and so on. AI is in every area of human life, naming a few it is into gaming, language processing, speech recognition, expert system, vision system, hand writing recognition, intelligence robots, financial transactions and what not, every activity of human life has become a subset of AI. In spite of numerous uses, AI can also used for destroying the human life, that is the reason human inference is required to monitor the AI activities. Cybercrime has become commonplace, with regular news coverage. It is a problem that affects the whole world, not just one country. Without solid security measures, AI is pointless since it is easily accessible to others. Hacker-led cyber attacks have posed a significant danger to governments, banks, and global corporations. Hackers exploit a large volume of individual and organisational data, posing a significant danger to the cyber world. In this regard, research in the fields of AI and cyber security has grown in importance in recent years, and it will continue to do so indefinitely since it is a dynamic and sensitive topic related to human existence.

Keyword: artificial intelligence , cyber crime, cyber security,

INTRODUCTION

Artificial Intelligence (AI) refers to the development of computer systems capable of performing tasks that typically require human intelligence. These tasks include learning from experience, reasoning, problem-solving, language understanding, perception, and even creativity. AI aims to create machines that can mimic or exceed human cognitive abilities, offering vast potential in various fields such as healthcare, finance, robotics, transportation, and beyond.

AI technologies are driven by algorithms, machine learning (ML), and data processing. Machine learning, a subset of AI, enables systems to improve and adapt autonomously by analyzing large datasets and recognizing patterns. Over the years, AI has rapidly evolved, moving from theoretical research to real-world applications that shape industries and everyday life.

Artificial intelligence (AI) plays a significant role in both enhancing cybersecurity and contributing to cybercrime. While AI offers powerful tools for defending against cyber threats, it is also being used by cybercriminals to carry out more sophisticated attacks. Here's a breakdown of AI's dual role in this context:

AI's Role in Cybercrime (Offensive Use by Cybercriminals):

1. **Automated and Scalable Attack**s: AI enables cybercriminals to automate large-scale attacks,

[73] Research Scholar at Chaudhary Devi Lal University, Sirsa, India.
[74] LLM Scholar from Chhaju Ram Law College, Hisar, India.

allowing them to target many victims simultaneously with minimal human intervention. Techniques like AI-powered bots can scan networks for vulnerabilities, execute phishing campaigns, or launch Distributed Denial of Service (DDoS) attacks more efficiently than manual efforts.

2. **Advanced Phishing and Social Engineering**: AI enhances phishing attacks by analyzing vast amounts of personal data to craft more personalized, convincing messages. AI systems can mimic human communication patterns, making phishing emails or social engineering attempts much harder to detect. This leads to a higher success rate for attacks that aim to steal sensitive information or login credentials.

3. **Sophisticated Malware Creation**: AI can assist in the development of malware that adapts and evolves based on the target environment. AI-enhanced malware can evade traditional security measures by learning from its surroundings and adjusting its behavior to avoid detection. Examples include polymorphic malware, which changes its code to elude antivirus systems, and ransomware that selectively targets high-value files for encryption.

4. **AI-Powered Exploits and Hacking Tools:** Cybercriminals use AI-based tools to perform reconnaissance, identify weak points in a system, and exploit vulnerabilities faster than humans. These tools can discover zero-day vulnerabilities, enabling attackers to infiltrate systems before patches are available. AI also accelerates the process of brute force attacks on passwords by rapidly testing combinations or analyzing user habits to guess credentials.

5. **Deepfakes and Synthetic Identity Fraud**: AI-generated deepfakes—realistic fake videos or audio recordings—are used for impersonation, fraud, or disinformation. Cybercriminals can manipulate deepfake technology to trick individuals, commit fraud, or even blackmail organizations by impersonating high-profile figures. Additionally, AI can generate synthetic identities that combine real and fabricated information, making it harder for financial institutions or security systems to detect fraudulent activities.

6. **AI-Driven Data Poisoning**: AI systems are vulnerable to "data poisoning" attacks, where malicious actors corrupt the datasets used to train AI models. By feeding incorrect or biased data into the training process, cybercriminals can manipulate AI models to make faulty decisions, such as misclassifying malware as benign or overlooking malicious activity.

7. **AI for Reconnaissance and Targeting**: AI systems can sift through massive amounts of publicly available data to build detailed profiles of potential targets. This intelligence can be used to design more effective attacks tailored to specific individuals or organizations, such as business email compromise (BEC) or spear-phishing attacks targeting high-value executives.

AI in Cybersecurity (Defensive Role):

1. **Threat Detection and Response:** AI can help identify and respond to threats faster than traditional methods. AI algorithms analyze vast amounts of data in real-time to detect anomalies, suspicious behavior, or known attack patterns. It can automatically flag or block potential threats before they cause harm.

2. **Behavioral Analysis:** AI is increasingly used for behavioral analysis in cybersecurity. By monitoring user activity, AI systems can identify abnormal patterns that may indicate an attack or insider threat. This helps in detecting threats that might bypass rule-based systems.

3. **Automated Incident Response:** AI can automate certain aspects of incident response, such as isolating infected systems, stopping ongoing attacks, and remediating vulnerabilities. This reduces the time it takes to mitigate damage from cyberattacks and helps organizations recover more quickly.

4. **Predictive Analytics:** AI's predictive capabilities allow security teams to anticipate future attacks by identifying emerging threats based on historical data. This proactive approach helps organizations to prepare for potential risks before they escalate into real attacks.

5. **Vulnerability Management:** AI can help in scanning systems for vulnerabilities more accurately and efficiently than human-led efforts. It can prioritize critical vulnerabilities and recommend patching schedules, allowing organizations to focus on the most significant risks.

6. **Fraud Detection:** In financial services and online transactions, AI is used to detect fraudulent activities by analyzing transaction patterns. AI systems can identify suspicious transactions, account takeovers, and other fraudulent activities with greater precision.

7. **Enhanced Identity and Access Management:** AI-based systems can enhance identity verification processes, including the detection of anomalies in login attempts and multi-factor authentication. AI can detect if a login attempt is legitimate based on factors such as user behavior, location, and device type.

Challenges:

- **AI Arms Race:** As AI becomes more advanced, both cybercriminals and security professionals are engaged in a technological arms race. Criminals are constantly finding new ways to exploit AI, while cybersecurity experts are working to develop countermeasures.

- **False Positives and Bias:** AI systems can generate false positives, overwhelming security teams with alerts that may not be actual threats. Additionally, biased AI models might overlook certain threats or unintentionally prioritize the wrong risks.

- **AI Attacks on AI Systems (Adversarial AI):** AI models themselves are targets. Adversarial attacks manipulate AI models by introducing subtle inputs that cause them to make incorrect decisions, like misidentifying a threat or classifying malicious activity as benign.

CONCLUSION

- Artificial intelligence represents both an opportunity and a challenge in the realm of cybersecurity. On one side, AI enhances the ability to detect, respond to, and prevent cyber threats by automating security processes, identifying patterns, and predicting future attacks. It allows organizations to scale their defenses in ways that were previously impossible and helps mitigate the increasingly sophisticated tactics employed by cybercriminals.

- However, the rise of AI also gives cybercriminals access to unprecedented capabilities, enabling them to launch highly targeted, efficient, and adaptive attacks. AI allows criminals to automate large-scale operations, create personalized phishing schemes, develop intelligent malware, and evade traditional security measures. Moreover, the use of AI in adversarial attacks, deepfakes, and data poisoning adds new layers of complexity to the cybersecurity landscape.
- The challenges posed by AI in cybercrime include the potential for an "AI arms race" between attackers and defenders, the exploitation of AI vulnerabilities, and the lack of skilled professionals who understand both AI and cybersecurity. Moreover, ethical concerns about biased AI systems, adversarial attacks, and the misuse of AI technologies further complicate the situation.
- To combat the growing threats posed by AI-driven cybercrime, organizations must:
- **Adopt AI-based security solutions** that can anticipate and respond to evolving threats in real-time.
- **Invest in the continuous development of AI models** to enhance their robustness and resilience against adversarial attacks.
- **Close the AI skills gap** by training more professionals who can understand and mitigate AI-related threats.
- **Collaborate with regulators** to create frameworks that hold both attackers and defenders accountable in the age of AI-driven crime.
- In the end, the future of cybersecurity will depend on a delicate balance between leveraging AI's potential for defense and mitigating the risks it poses when used for malicious purposes. Organizations must stay ahead of cybercriminals by continuously improving AI security measures and remaining vigilant against emerging AI-driven attack strategies.

*****

SOCIO-LEGAL IMPLICATION OF AI INTEGRATION IN COURTS OF JUSTICE

Mamta Devi[75] and Dr. Vikas Poonia[76]

ABSTRACT

The integration of Artificial Intelligence (AI) into judicial systems is reshaping the landscape of justice, offering a range of potential benefits but also raising complex socio-legal concerns. On one hand, AI enhances access to justice by streamlining legal procedures, improving case management, and predicting case outcomes more efficiently. These systems can help courts address backlogs and promote consistency in judgments. However, serious challenges arise. ***Algorithmic bias*** *remains a critical issue, as AI systems may unintentionally perpetuate existing prejudices, threatening the fairness of judicial outcomes. Moreover, the lack of transparency in AI decision-making processes can erode trust in the legal system, with questions surrounding the accountability of AI-generated judgments and the ethical implications of non-human decision-makers. Additionally, the use of AI raises significant privacy concerns, as sensitive personal data may be processed without adequate safeguards. The impact on the legal profession also cannot be overlooked, with AI automating tasks traditionally performed by lawyers and legal researchers, potentially displacing jobs while creating new skills gaps. These socio-legal implications highlight the need for robust regulatory frameworks and ethical oversight to ensure that AI strengthens, rather than undermines, the core principles of justice. A balance must be struck between leveraging the technological advantages of AI and protecting fundamental rights to ensure that the judicial system remains fair, transparent, and human-centered. Main objective of the study: 1. Analyze the potential benefits of AI in enhancing judicial efficiency, improving access to justice, and reducing human bias. 2. Identify the key challenges posed by AI, including algorithmic bias, accountability, transparency, and privacy concerns. Doctrinal research methodology will be adopted for further research.*

Keywords: Artificial Intelligence, access to justice, algorithmic bias, accountability, legal ethics.

INTRODUCTION

The integration of Artificial Intelligence (AI) in judicial systems is becoming a global trend. In India, the judiciary faces challenges such as case backlogs, delays, and limited access to justice, making the use of AI a potentially transformative solution. While AI promises to enhance efficiency and streamline the judicial process, it raises concerns about transparency, accountability, data privacy, and the role of human discretion. This study argues that a cautious approach, with adequate safeguards, is essential for successful AI integration into India's judiciary.

The incorporation of technology in judicial systems has evolved gradually, with each advancement aiming to address inefficiencies and improve access to justice. Artificial Intelligence (AI), with its ability to process vast amounts of data and predict outcomes, represents the latest phase in this evolution. Although the global adoption of AI in courts began earlier in countries like the United States and China, India is making strides through pilot programs and institutional reforms aimed at using AI to tackle the judiciary's challenges. The history of AI in Indian courts must be viewed as part of the

[75] LHP College of Law, Sirsa, India.
[76] Department of Law, Ch. Devi Lal University, Sirsa, India.

larger technological evolution of the justice system, beginning with the computerization of records and the e-Courts project.

EVOLUTION OF TECHNOLOGY IN THE INDIAN JUDICIARY

1. Early Computerization of Judicial Processes (1990s – 2000s)

In the 1990s, Indian courts began adopting Information and Communication Technology (ICT) to digitize case records and manage administrative processes.

By the early 2000s, some high courts experimented with digital case filing systems, allowing advocates to track case status through online portals. However, the adoption remained uneven across courts due to limited infrastructure and connectivity.

2. Launch of the E-Courts Mission Mode Project (2005 – Ongoing)

Recognizing the need to modernize the judiciary, the Government of India launched the **e-**Courts Mission Mode Project under the National e-Governance Plan (NeGP) in 2005.

The primary goal of this project was to digitize case records, automate court processes, and develop an online interface for litigants and lawyers.

Phase I (2005-2015**)** focused on establishing computer infrastructure in district and subordinate courts. Phase II (2015-2023) aimed to enhance access to information through mobile apps and online portals, paving the way for future AI adoption.

THE EMERGENCE OF AI IN THE INDIAN JUDICIARY

1. Introduction of AI Tools (2018 – 2020)

AI technologies started to gain attention in the Indian judiciary around 2018, following the success of international initiatives in predictive analytics and online dispute resolution (ODR).

The National Informatics Centre (NIC) and the Supreme Court of India began exploring AI-powered solutions to enhance legal research and improve court efficiency.

2. SUPACE: A Landmark Initiative (2021)

In 2021, the Supreme Court of India launched the **SUPACE** (Supreme Court Portal for Assistance in Court Efficiency) project, marking the first formal use of AI technology at the highest judicial level.

SUPACE is designed to assist judges with legal research by summarizing case laws, extracting relevant data, and recommending judgments.

This initiative aims to reduce the workload on judges, especially in cases involving complex legal precedents.

KEY DEVELOPMENTS IN AI INTEGRATION (2021 – PRESENT)

1. AI-Powered Transcription Services

The Delhi High Court implemented AI-based transcription services in 2023, enabling real-time recording and transcription of court proceedings. This technology improves transparency and reduces the reliance on manual note-taking by court staff.

2. Predictive Analysis for Case Prioritization

Some state high courts, including the Bombay High Court, have piloted AI-based predictive tools to identify and prioritize urgent cases, such as bail hearings and public interest litigations (PILs). These efforts aim to address India's chronic problem of case backlog, which continues to overwhelm the judiciary.

3. Online Dispute Resolution (ODR) Platforms

During the COVID-19 pandemic, courts increasingly relied on virtual hearings and ODR platforms. AI tools integrated into these platforms facilitate automated dispute resolution for smaller claims, such as consumer complaints and traffic violations.

CHALLENGES IN AI ADOPTION

1. Infrastructure Gaps and the Digital Divide

While AI is gaining ground in higher courts, many district and rural courts lack the infrastructure needed for AI integration. Limited access to the internet and electricity poses a significant barrier to uniform adoption across India.

2. Public Trust and Resistance from Legal Professionals

Judges and lawyers are cautious about AI, fearing that technology could *undermine* ***judicial discretion*** *and* ***replace human empathy*** with mechanical decision-making. This skepticism highlights the need for training programs and awareness campaigns to build trust in AI tools.

3. Ethical and Legal Frameworks

India currently lacks specific regulations governing the use of AI in judicial systems. The absence of clear ***legal and ethical frameworks*** raises concerns about the accountability, transparency, and fairness of AI-generated decisions.

THE WAY FORWARD

1. Phase-Wise Implementation of AI Tools

Experts suggest a phased approach to AI integration in courts, beginning with administrative tasks such as case scheduling and legal research. This will allow stakeholders to understand AI's limitations and refine its use before expanding it to decision-making processes.

2. Collaboration with International Partners

India can learn from the experiences of ***Estonia, China, and the United States***, which have pioneered AI tools in courts. Collaborative efforts with these countries will help India develop ***best practices*** *and* ***ethical guidelines***.

3. Capacity Building and Training

To ensure successful AI adoption, the judiciary must invest in ***training programs for judges, lawyers, and court staff***. Capacity building will ensure that legal professionals can leverage AI tools effectively while maintaining the human element in judicial decision-making.

I. The Role of AI in Indian: AI can help reduce delays by streamlining administrative tasks such as case scheduling, docket management, and legal research.

2. Predictive Justice: AI-based systems can forecast case outcomes, enabling judges to prioritize urgent matters.

3. Legal Research and Documentation: AI-powered platforms can analyze precedents, case laws, and statutes more efficiently than traditional methods.

4.Virtual Courts: AI can support online dispute resolution (ODR) systems, which have gained prominence during the COVID-19 pandemic.

Example: The Delhi High Court recently piloted AI-based transcription services, automatically recording court proceedings in real time

LEGAL IMPLICATIONS IN THE INDIAN CONTEXT

1. Bias and Fairness in AI Systems

AI systems reflect the data on which they are trained. If these datasets include biased judgments or discriminatory practices, the AI might perpetuate these biases. Given India's complex socio-economic and caste-based realities, biased algorithms could disproportionately affect marginalized communities, such as Scheduled Castes, Scheduled Tribes, and minorities.

Case Example:

If AI is used in bail decisions, there is a risk that biases in the system could deny bail to economically weaker sections or historically marginalized groups.

2. Accountability and Judicial Discretion

The principle of natural justice requires that human judges have the final say in legal matters. Delegating decision-making to AI risks diluting judicial accountability. In India, public trust in the judiciary depends on human discretion, empathy, and contextual understanding—qualities that AI cannot replicate. The question remains: Who will be responsible if an AI tool recommends an incorrect judgment?

3. Admissibility of AI-Generated Evidence

Indian courts must determine whether AI-generated insights meet the evidentiary standards of the Indian Evidence Act, 1872. For example, evidence collected or analyzed by AI tools must be scrutinized for reliability, fairness, and authenticity. AI-based forensic tools, if not regulated properly, could lead to wrongful convictions.

In India, the Supreme Court has introduced AI tools like ***SUPACE (Supreme Court Portal for Assistance in Court Efficiency)*** to assist in judicial processes. SUPACE helps judges by organizing

relevant facts and case laws efficiently, reducing delays caused by large backlogs. However, the system does not make decisions independently; instead, it supports judges with legal research and document summarization to enhance their efficiency.

While there aren't specific judgments rendered solely by AI, legal technology tools like SUPACE are being piloted in select high courts (e.g., Bombay and Delhi) for cases involving criminal matters. This reflects India's move towards integrating AI for legal research and analysis. Additionally, precedents such as ***State of Maharashtra v. Praful Desai (2003)***, which allowed video conferencing for evidence recording, paved the way for using advanced technology in courts, indirectly contributing to the acceptance of AI-driven tools.

Moreover, cases like ***Justice K.S. Puttaswamy v. Union of India (2017)*** highlight privacy concerns crucial to AI applications. With the growing reliance on AI systems processing sensitive legal data, the intersection between privacy rights and legal tech is becoming increasingly relevant. These advancements suggest that the Indian judiciary is carefully balancing technological innovation with human oversight and ethical considerations.

SOCIAL IMPLICATIONS OF AI INTEGRATION IN COURTS

1. Access to Justice

AI can improve access to legal services through chatbots and online dispute resolution systems that assist citizens with legal queries and small claims. This would be particularly helpful in rural areas where access to courts is limited. However, the digital divide limited internet penetration and lack of digital literacy—could exclude vulnerable populations, such as tribal communities or the elderly, from accessing AI-enabled justice systems.

2. Public Trust in AI-Driven Justice

AI's objectivity might appeal to some citizens, but others could view it as a dehumanizing force. Public trust in courts in India is closely tied to the personal and empathetic role of judges. A completely automated or AI-driven process could create fear that justice is reduced to mere algorithms, undermining the judiciary's moral legitimacy.

3. Impact on Legal Professionals

While AI can reduce routine legal work, it may also disrupt traditional legal professions. Junior lawyers, clerks, and paralegals, who rely on drafting and documentation tasks, might find fewer employment opportunities. However, new roles such as legal data analysts and AI ethics expert are likely to emerge, requiring reskilling.

ETHICAL AND REGULATORY FRAMEWORKS

1. Developing AI Regulations in India

Currently, India lacks specific laws governing AI in the judiciary. The Personal Data Protection Act, 2019 offers some guidance, but comprehensive legal frameworks are required to address the ethical and

legal implications of AI in courts. It is crucial to ensure that AI systems used in courts are auditable, transparent, and free from bias.

2. Balancing Automation with Human Oversight

The judiciary must strike a balance between using AI for efficiency and ensuring human judges retain control over decisions. AI tools should act as assistants, not replacements. The final judgment in legal matters must rest with a human judge, in line with the principles of judicial discretion.

CHALLENGES AND FUTURE PROSPECTS

1. Resistance to Change

The adoption of AI faces resistance from various stakeholders, including judges and lawyers, who may fear that technology will undermine their authority or expertise. Training programs and awareness campaigns are essential to build acceptance among the judiciary and legal fraternity.

2. Need for Infrastructure Development

AI integration requires significant investments in digital infrastructure and capacity building. Rural courts and lower judiciary must be equipped with the necessary technology to ensure uniform implementation across the country.

3. Pilot Programs and Experimentation

India should follow a phased approach to AI adoption, starting with pilot programs in specific areas, such as small claims or traffic violations. These pilot projects can help policymakers identify challenges and refine AI applications before full-scale implementation.

Here's a detailed comparative analysis of AI integration in courts across India, Singapore, UK, USA, and China.

1. India

AI Usage: AI tools like SUPACE assist in case management by streamlining data analysis and helping judges access relevant case laws quickly.

Focus: SUPACE and other tools emphasize judicial support without replacing human decision-making. The Indian judiciary insists that AI must remain an aid rather than a determinant in legal decisions.

Challenges: India grapples with privacy concerns (e.g., under the Personal Data Protection Bill) and ensuring AI use is free from bias. The judicial system has begun pilots in criminal cases at Bombay and Delhi High Courts to measure effectiveness.

2. Singapore

AI Usage: Singapore's Community Justice and Tribunals System (CJTS) employs AI to automate small claims cases and handle case filings online. Predictive analytics is also being explored to forecast case outcomes.

Focus: Singapore leads in creating online dispute resolution (ODR) platforms that leverage AI, ensuring quicker and more cost-effective outcomes. Judges remain at the center of legal decisions, ensuring human oversight in AI operations.

Challenges: The main concern lies in balancing efficiency and transparency while addressing ethical concerns regarding predictive tools.

3. United Kingdom

AI Usage: AI systems are used to manage case scheduling, documentation, and legal research. The judiciary has issued AI guidance documents to ensure legal professionals understand the boundaries and potential risks of AI in court operations.

Focus: Emphasis is placed on judicial ethics and privacy protection, particularly ensuring that confidential information is not entered into AI tools. The UK remains cautious about the extent of AI integration into judicial reasoning.

Challenges: Concerns about bias, data privacy, and maintaining judicial independence are prominent. Human judgment continues to be prioritized over AI suggestions.

4. United States

AI Usage: The U.S. uses AI-driven risk assessment tools to assist in bail and sentencing decisions. These algorithms evaluate factors like recidivism risk, helping judges in criminal cases.

Focus: AI is more involved in decision-making than in countries like India or the UK, but this has sparked debates about the transparency and accountability of such systems.

Challenges: Criticism has arisen around algorithmic bias and potential violations of due process, especially when AI-based recommendations are not clearly explainable to defendants.

5. China

AI Usage: China has implemented AI-powered "Smart Courts," where AI tools provide verdict recommendations, predict case outcomes, and even automate parts of trials.

Focus: AI plays a more central role in judicial decision-making, with fewer constraints compared to other countries. China's system supports judges in administrative and legal work, speeding up processes significantly.

Challenges: There is little discussion about judicial independence, as the AI-based judicial system is closely aligned with the government's push for legal reforms. Ethical concerns around fairness and bias are less emphasized compared to Western counterparts.

CONCLUSION

The integration of AI in the Indian judiciary offers exciting opportunities to enhance efficiency, reduce case backlogs, and improve access to justice. However, the socio-legal challenges—bias, accountability, public trust, and the digital divide—must be carefully managed. AI should serve as an augmented tool that complements human judgment, not replaces it. A cautious approach, guided by

ethical regulations and human oversight, is essential to ensure that AI strengthens the judiciary without compromising fairness, transparency, or public confidence.

India's journey toward AI-enabled courts must be guided by the twin principles of technology with a human touch and justice for all, ensuring that the benefits of AI are distributed equitably and aligned with constitutional values.

REFERENCES

- Indian Judiciary Annual Report 2024. Supreme Court of India.
- E-Courts Mission Mode Project, Government of India.
- Personal Data Protection Act, 2019.
- Yadav, S., & Sharma, A. (2022). "AI and Legal Ethics: A Study of Indian Courts." International Journal of Law & Technology, 14(1), 34-56.
- Bansal, R. (2021). "Can AI Replace Judges? Indian Perspectives on AI in Judicial Systems." Journal of Law & Policy, 12(2), 102-118.

Primary Sources

- Department of Justice, E-Courts Mission Mode Project, Government of India, available at: <https://ecourts.gov.in> (last visited October 17, 2024).
- Supreme Court of India, Launch of SUPACE: AI in Judicial Functioning, 2021.
- Government of India, The Personal Data Protection Bill, 2019, PRS Legislative Research, available at: <https://prsindia.org> (last visited October 17, 2024).

Journal Articles

- Bansal, R., "Can AI Replace Judges? Indian Perspectives on AI in Judicial Systems," (2021) 12(2) Journal of Law & Policy 102.
- Yadav, S. and Sharma, A., "AI and Legal Ethics: A Study of Indian Courts," (2022) 14(1) International Journal of Law & Technology 34.

Reports and Official Documents

- NITI Aayog, National Strategy for Artificial Intelligence: AIforAll, Government of India, 2018, available at: <https://www.niti.gov.in> (last visited October 17, 2024).
- OECD, AI in the Public Sector: Comparative Judicial Systems, Organisation for Economic Co-operation and Development, 2021, available at: <https://www.oecd.org> (last visited October 17, 2024).
- National Judicial Data Grid, Statistical Reports on Case Pendency and Clearance Rates, available at: <https://njdg.ecourts.gov.in> (last visited October 17, 2024).

News Articles

- “Delhi High Court Uses AI for Real-Time Transcription,” The Hindu, February 12, 2023. “SUPACE: AI Comes to the Supreme Court of India,” Indian Express, March 5, 2021.

*****

E-JUSTICE: THE ROLE OF POLICE IN INVESTIGATING CYBER OFFENSES

Vakeel[77]

ABSTRACT

In today's digital landscape, the increasing prevalence of cyber offenses presents significant challenges for law enforcement agencies dedicated to upholding public safety. Cybercrime includes a broad array of illicit activities conducted online, such as identity theft, hacking, online fraud, and cyberbullying. As these crimes grow more sophisticated, police forces must adapt their strategies and techniques to effectively investigate and respond to this evolving threat. This paper explores the multifaceted role of police in addressing cyber offenses, focusing on the complexities of digital evidence, jurisdictional hurdles, and the rapid pace of technological change. The research begins by examining how the nature of crime has transformed in the digital age. Unlike traditional crimes, cyber offenses often cross national borders, complicating law enforcement efforts. Issues related to jurisdiction arise when offenders operate from different countries, highlighting the need for international cooperation and coordination. This paper discusses existing frameworks for collaboration, including mutual legal assistance treaties (MLATs) and partnerships with global organizations, which are essential for effective cybercrime investigations. Finally, the paper underscores the significance of community engagement and public awareness in preventing cyber offenses. Law enforcement agencies are increasingly partnering with educational institutions and community organizations to promote cybersecurity awareness, equipping individuals with the knowledge necessary to safeguard themselves against digital threats. In conclusion, this study offers a comprehensive overview of the role of police in investigating cyber offenses. As the landscape of cybercrime continues to evolve, law enforcement must refine its strategies, enhance training, and adopt technological advancements to effectively address these challenges. By fostering international collaboration and prioritizing ethical considerations, police can uphold justice in the digital realm, contributing to a safer online environment for all. This research aims to inform policymakers, law enforcement leaders, and the public about the critical challenges and strategies involved in tackling the urgent issue of cybercrime.

Keywords: Cybercrime, Cyber Security, E-Justice, Digital.

INRODUCTION

The digital revolution has dramatically altered the way we communicate, work, and live, but it has also introduced new forms of crime. Cybercrime, encompassing activities like hacking, phishing, identity theft, and cyberbullying, has emerged as one of the most significant challenges for law enforcement agencies globally. With the rise of the internet and the increasing reliance on digital platforms, cyber offenses have become pervasive, complex, and transnational in nature. This evolution has placed unprecedented pressure on the police, who must now not only address traditional forms of crime but also adapt to new methodologies of investigation in the digital realm. E-Justice, a term referring to the use of electronic means in the administration of justice, plays a crucial role in modern law enforcement, particularly in the investigation of cyber offenses. The role of police in investigating cybercrime is critical, as they serve as the first line of defense in both preventing and responding to these crimes.

This research paper examines the evolving role of law enforcement in the investigation of cyber offenses. It explores the challenges police face, the tools and techniques employed, the legal frameworks

[77] Assistant Professor at Department of Law, Ch. Devi Lal University, Sirsa, India.

governing cybercrime investigations, and the collaboration required at national and international levels. Additionally, it will discuss the future of policing in the context of rapidly evolving cyber threats and the integration of e-justice in this paradigm.

THE NATURE OF CYBER OFFENSES

Defining Cybercrime

Cybercrime refers to criminal activities that are carried out using computers, digital networks, or the internet. These crimes can be broadly categorized into two types:

1. **Computer-targeted crimes**: These include hacking, distributed denial-of-service (DDoS) attacks, and malware infections, where the computer itself is the target.
2. **Computer-assisted crimes**: In these cases, computers are used as tools to commit traditional crimes like fraud, theft, or child exploitation.

While some cybercrimes, like hacking or malware distribution, are unique to the digital domain, others, such as identity theft, extortion, or harassment, are merely extensions of pre-existing criminal behaviors adapted for the digital world. The anonymity offered by the internet, combined with the global nature of cyberspace, has created fertile ground for cybercriminals.

The Growth of Cyber Offenses

Cybercrime has grown exponentially over the past few decades. The rapid digitalization of economies and the proliferation of smartphones and internet-connected devices have created a vast, vulnerable landscape. The sheer number of devices and users online, combined with the lack of stringent cybersecurity protocols in many sectors, has led to a massive increase in the frequency and sophistication of cyber offenses.

A report from Cybersecurity Ventures predicts that the cost of cybercrime globally will reach $10.5 trillion annually by 2025, representing an increase of 15% year over year. This makes cybercrime more profitable than the global illegal drug trade, and a threat that cannot be ignored by governments, businesses, and individuals alike.

THE ROLE OF POLICE IN CYBERCRIME INVESTIGATION

Traditional Law Enforcement vs. Cybercrime Investigation

Historically, police forces have dealt with crimes that are physical in nature—robberies, homicides, assaults, etc. However, with the digital transformation of society, law enforcement agencies are now required to expand their expertise into the domain of digital forensics, cybersecurity, and information technology. The traditional skillsets of a police officer—surveillance, interrogation, physical evidence collection—are insufficient when dealing with a faceless, often transnational cybercriminal.

The role of police in investigating cyber offenses now involves identifying and collecting digital evidence, tracing the origins of online activities, and using advanced technologies to break through encryption or anonymization tools used by criminals. Furthermore, the borderless nature of the internet

complicates matters as cybercriminals often operate from different jurisdictions, making international cooperation essential.

Investigative Tools and Techniques

In order to investigate cybercrime effectively, police forces need specialized tools and skills, including:

1. **Digital Forensics**: The process of recovering, analyzing, and preserving electronic data, such as emails, chat logs, IP addresses, and digital footprints. Forensic investigators often extract evidence from computers, smartphones, and other devices.
2. **Cyber Intelligence Gathering**: Police use various techniques to monitor the dark web, social media platforms, and other online spaces where cybercriminals operate. This requires not only technical expertise but also the ability to infiltrate and gather intelligence from hacker communities.
3. **Tracking and Tracing**: Cybercriminals often use methods such as VPNs, proxies, and the Tor network to hide their identities. Police employ methods such as IP address tracking, metadata analysis, and exploiting weaknesses in anonymization to trace these individuals.
4. **Encryption Breaking**: As encryption technologies have advanced, so have the challenges they pose to law enforcement. Police forces often work with cybersecurity experts or use tools designed to break or bypass encryption to access evidence.
5. **Artificial Intelligence (AI) and Automation**: AI has begun playing a role in identifying patterns and predicting cyberattacks. Automated systems can help law enforcement analyze large volumes of data quickly and efficiently, identifying potential criminal activities in real-time.

LEGAL AND REGULATORY FRAMEWORKS

Cybercrime Laws

The investigation of cyber offenses is governed by a complex framework of national and international laws. These laws aim to define what constitutes cybercrime, outline the powers of law enforcement in investigating such crimes, and ensure the protection of citizens' privacy and rights in the digital domain.

Many countries have introduced cybercrime-specific legislation. For instance, the **Computer Fraud and Abuse Act (CFAA)** in the United States criminalizes unauthorized access to computer systems, while the **General Data Protection Regulation (GDPR)** in the European Union sets strict rules on data privacy, influencing how police can handle digital evidence.

However, a significant challenge is the disparity in laws across different jurisdictions. What may be considered a cybercrime in one country might not be classified as such in another, making international cooperation difficult.

International Cooperation and Agencies

Given the transnational nature of cybercrime, international cooperation is essential. Organizations like **Interpol**, the **European Cybercrime Centre (EC3)**, and **UNODC** (United Nations Office on Drugs

and Crime) facilitate cooperation between nations in sharing intelligence, training law enforcement personnel, and coordinating joint operations.

One significant international legal framework is the **Budapest Convention on Cybercrime**, the first international treaty seeking to address cybercrime by harmonizing national laws, improving investigative techniques, and fostering international cooperation.

Despite these efforts, challenges remain, including varying levels of law enforcement capabilities across countries and differing attitudes toward internet governance and surveillance.

CHALLENGES IN CYBERCRIME INVESTIGATION

Technological Complexity

The rapidly evolving nature of technology presents a significant challenge to police forces. Cybercriminals are constantly adapting, using more sophisticated methods such as ransomware, cryptojacking, and deepfakes to evade detection. Law enforcement agencies must continuously update their knowledge and tools to keep pace.

Jurisdictional Issues

As cyber offenses often cross national borders, jurisdictional disputes frequently arise. A cybercriminal operating in one country can target victims in multiple other countries, complicating the investigation. Police forces may face difficulties in obtaining digital evidence stored in foreign servers or pursuing suspects located abroad due to differences in legal systems.

Resource Constraints

Cybercrime investigation requires specialized skills and expensive technology, which many police departments, particularly in developing countries, may not have. Furthermore, as cybercrime continues to rise, law enforcement agencies are often overwhelmed by the volume of cases.

Privacy Concerns

Balancing the need for security with the protection of individual privacy rights is another challenge. Law enforcement agencies must adhere to legal standards when accessing personal data or intercepting communications. Overreach can lead to violations of privacy, eroding public trust.

FUTURE DIRECTIONS AND E-JUSTICE

Enhanced Training and Capacity Building

To effectively combat cybercrime, police forces must invest in continuous education and training. Law enforcement officers need to be skilled in digital forensics, encryption technologies, and cyber intelligence gathering. Many countries are now incorporating cybercrime investigation modules into police training academies, while others are forming specialized cybercrime units.

Public-Private Partnerships

As much of the infrastructure targeted by cybercriminals is privately owned, such as financial institutions and cloud service providers, collaboration between law enforcement and the private sector

is critical. Information sharing agreements, joint task forces, and cybersecurity frameworks that bridge the gap between public and private entities are essential in the fight against cybercrime.

Advancing E-Justice

E-Justice refers to the use of electronic systems to improve the administration of justice. For law enforcement, this means leveraging technology not only for the investigation of cybercrimes but also for streamlining judicial processes, including the handling of evidence, filing of reports, and communication with prosecutors and judges.

By implementing e-justice solutions, police forces can improve the speed and efficiency of cybercrime investigations, enhance transparency, and ensure that digital evidence is handled securely.

CONCLUSION

The rise of cyber offenses has significantly transformed the landscape of law enforcement, demanding that police forces adapt to new technologies and methodologies in their investigations. The role of the police in investigating cybercrime involves more than just technical expertise; it requires international cooperation, legal sophistication, and a delicate balance between security and civil liberties.

With the integration of e-justice and advanced digital tools, the police are better equipped to meet the challenges posed by cybercriminals. However, this evolution is ongoing, and law enforcement agencies must continue to invest in training, technology, and partnerships to remain effective in the fight against cybercrime.

*****

REFERENCES

1. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
2. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
3. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Forensics: An Introduction*. Routledge.
4. Goodman, S. E., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, 10(2), 139-223. doi:10.1093/ijlit/10.2.139
5. Grabosky, P. (2007). The Internet, Technology, and Organized Crime. *Asian Journal of Criminology*, 2(2), 145-161. doi:10.1007/s11417-007-9030-2
6. Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486. doi:10.1177/0894439311422681
7. Europol (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Europol.
8. United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive Study on Cybercrime*. United Nations.

9. INTERPOL (2021). *Cybercrime*. Available at: https://www.interpol.int/en/Crimes/Cyb ercrime
10. Council of Europe (2001). *Convention on Cybercrime (Budapest Convention)*. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention
11. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Elsevier.
12. U.S. Department of Justice (2020). *Best Practices for Seizing Electronic Evidence*. DOJ Cybercrime Lab.
13. National Institute of Standards and Technology (NIST) (2020). *NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response*. NIST.
14. European Parliament (2020). *Study on the Implementation of the General Data Protection Regulation (GDPR) and Its Impact on Cybercrime Investigations*. Available at: https://www.europarl.europa.eu/
15. Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press

*****

PROTECTING THE UNSEEN – DEALING WITH CYBER CRIMES AFFECTING CHILDREN

Vishakha Agarwal[78] and Yogita C Javkar[79]

ABSTRACT

In recent years, digitalisation has become the new normal. From communicating and shopping to banking and other daily activities, everything happens at our fingertips. This increases the use of technology for all age groups, especially children. While digital platforms provide various opportunities, they also expose vulnerable groups to multiple types of cyber threats. Cyberbullying, internet exploitation, cyberstalking, identity theft, etc are some of the examples. With features like anonymity and the vast reach of the internet, it is easier to target children that are below the age of eighteen due to their lack of maturity level and awareness. Social media, gaming platforms, and artificial intelligence play a crucial role in cybercrimes as they expose children to privacy breaches, harassment, and inappropriate content which increases the need for improving security and parental supervision to protect children from exploitation. The existing literature shows that 36% of young people have experienced cyberbullying. In response, tech companies are enforcing strict content moderation policies, and schools are organizing anti-bullying programs to create awareness among students. However, the effectiveness of these measures in reducing cyberbullying remains a critical area for further research. Against this backdrop, the authors attempt to explore different cyber threats impacting children and highlight the connection between human rights and online safety. The paper is divided into two parts, Part one deals with the analysis of the various cyber threats faced by children, while part two offers suggestions that, if implemented, have the potential to significantly reduce the risks children face in the digital environment, promoting a balanced use of technology, and ensuring that children are better protected in the evolving digital environment.

INTRODUCTION

Digitalisation and the use of technology have become our backbone in today's generation. It has transformed the way we live, communicate, and interact. There is no doubt that it has brought various benefits and made our lives easy but it has created new opportunities for crime, especially towards vulnerable populations like children. Online offences targeting children have increased due to activities like cyberbullying online exploitation child pornography and identity theft. These threats attract children very easily due to their frequent use of social media platforms, online gaming, and educational websites which create an undetectable but significant danger. According to the National Crime Records Bureau (NCRB), 1,823 cases of cybercrimes against children were filed. It is essential to understand and fight back against these threats as children increasingly rely on the Internet for education, social interaction, and entertainment. There is a need for special attention because children are uniquely vulnerable in the digital space. Their innocence and lack of understanding of online dangers make them easy targets for cyber crimes. The introduction of stricter frameworks from legal, social, and technological sectors is essential to protect children online because traditional crime prevention methods are deficient in dealing with the challenges and anonymity of cyber crimes.

[78] Student at KLE Society's Law College, India.
[79] Student at KLE Society's Law College, India.

TYPES OF CYBER CRIMES AFFECTING CHILDREN

It is vital to list down the following types of cybercrimes affecting children to understand the root cause of cyber-crimes affecting children –

a) Cyberbullying: Cyberbullying is one of the most common forms of cybercrime impacting children. Digital platforms are used to harass, threaten, or humiliate a child. Statistics say that in 2022, 158 cases of cyberbullying were filed. It is different from traditional bullying because it follows children into their homes through mobile devices and computers. The effects of cyberbullying are highly dangerous as it can cause emotional and psychological harm like depression, anxiety, and even suicidal thoughts.

b) Child Pornography and Exploitation: The production, distribution, and consumption of child sexual abuse material is one of the most heinous forms of cybercrime. 1,171 cases of cyber pornography were filed in 2022. Child pornography violates the rights and dignity of children and fosters a global market of exploitation. The prohibition of such crimes is difficult despite rigid laws in many countries due to the easy availability of such material in the online market.

c) Online Predators: Features provided by the internet like speed, convenience, anonymity, etc are often misused by online harassers to target children. They begin by gaining the trust of the victims by pretending to be individuals who share similar interests before engaging in exploitation. Children unknowingly involve in harmful activities, inappropriate conversations, send explicit content or get manipulated for sexual exploitation leading to psychological issues like trauma, distrust, emotional damage, etc.

d) Identity Theft and Data Privacy: Children below the age of eighteen years are unaware of the nature and consequences of the activities they are involved in. Their active involvement in social media and gaming platforms is prominent daily. This allows them to share their personal information without being aware of the risks like data breaches and exploitation. Criminals can use a minor's identity to commit fraud, misuse bank statements, and participate in illegal activities resulting in long-term consequences affecting the child's future.

LEGAL FRAMEWORK FOR CHILD PROTECTION

It is essential to form a vigorous legal structure for child protection against cybercrime in the digital environment. This is because there was an overall increase of 8.73% in crimes against children which sums up to 1,62,449 cases in 2020. Let's have a look at the following elements and angles of the legal system in different regions –

i) Internationally, the United Nations Convention on the Rights of the Child (UNCRC) stresses the protection of children from exploitation and abuse in digital spaces. Optional Protocol on the Sales of Children, Child Prostitution, and Child Pornography tackles issues related to online child exploitation. Council of Europe's Convention on Cybercrime offers a framework for international cooperation in battling cybercrime offences against children.

ii) Most countries have introduced laws to protect children from cyber crimes. Laws like Child Protection Laws, Data Protection and Privacy Laws, and Cybercrime Laws are some examples that protect children from abuse, personal data and privacy online, and criminalize activities like online harassment, child pornography, and identity theft. Moreover, the Children's Online Privacy Protection Act (COPPA) in the United States demands that websites and online services must obtain parental consent before collecting personal information from children below 13. The Online Safety Bill in the United Kingdom enforces stricter rules and regulations on social media platforms to confirm child safety. The Protection of Children from Sexual Offences (POSCO) Act in India criminalizes the production, distribution, and possession of Child Sexual Abuse Material (CSAM). However, many nations lack in having exhaustive laws handling all types of cyber-crimes targeting children. Therefore, the legal system for child protection against cybercrime must be diverse including international standards, national legislation, and collaboration among various stakeholders so that a safer digital environment for children can be created.

LANDMARK CASES ADDRESSING CYBERCRIME AGAINST CHILDREN

State of Tamil Nadu v. K. Ramasamy (2019) in India dealt with issues of child pornography and supported the importance of legal provisions of Section 67B under the Information Technology Act, 2000 which prohibits the publishing and transmitting of child pornography. United States v. C.M. (2019) in the United States involved a minor who was accused of sending nude images of herself to peers where the court made judgements on the challenges relating to sexting among children handling issues of consent and child pornography laws. In R v. T (2007) in the United Kingdom the court's decisions were made on the use of online chat rooms to groom children for sexual exploitation which led to making legal guidelines for prosecuting digital sexual crimes involving minors. Similarly, various cases in Australia, Canada, and the European Union made a mark on issues relating to child pornography, child exploitation, etc.

TECHNOLOGICAL SOLUTIONS FOR PREVENTION

To prevent these cyber-crimes against children, it is necessary to make solutions in the technological aspects i.e., imposing parental control software for monitoring and restricting children's online activities, using the right amount of artificial intelligence and machine learning to identify and oppose cyber crimes relating to children, providing encryption and data privacy tools ensuring that sensible information like locations, identities, and images are not easily accessible to cyber bullies. Moreover, software like blockchain technologies, cyberbullying detection and prevention tools, tracking tools, VPNs, and digital footprint management tools must be introduced to verify identities of users in online environments, offer real-time monitoring of social media interactions, allow parents/guardians to track their child's real-time location, to create secure and encrypted connections for children, and help manage and reduce the amount of data that apps and websites collect from the users.

ROLE OF EDUCATIONAL INSTITUTIONS AND PARENTS

In addition to technological solutions, educational institutions and parents also play a vital role in a child's life that can help prevent and address cyber crimes against children. Their combination can form

a protective environment that helps children develop skills and awareness important to guide digital world safety.

Educational institutions must incorporate cyber safety into their programme so that responsible internet use, identifying cyber threats, and protecting personal data can be taught to children. Workshops and seminars must be conducted by professionals that can raise awareness among students, teachers, and parents about the risks of cybercrime. Students must be taught about these crimes age-appropriately i.e., younger students can learn about stranger danger online and older students can learn about phishing, sexting, and privacy settings. Schools must establish clear policies and protocols like anti-cyberbullying policies, acceptable use policies for school computers, mobile devices, and internet access, structured reporting system for cybercrime incidents to spread awareness of safe and appropriate online behaviour. Along with the students, teachers and counsellors must be trained on cyber safety so that they can identify signs of cyberbullying, online harassment, and online harassers and most essentially identify vulnerable students who may be victims of cybercrime. Schools must provide a safe online learning environment i.e., monitoring and ed-tech tools that can block harmful content, detect potential cyber threats, and recognise theft or exploitation of personal data. Partnerships with law enforcement and cybersecurity experts are another step that schools can take to update emerging cyber threats develop protocols and help students and parents to understand the real-world impact of cybercrime.

Children spend most of their time with parents at home which makes them responsible as well to preventing their child from cyber-crimes. Their active participation in online activities like supervising their children's online behaviour, the apps they use, the websites they visit, and the people they communicate with online, creates open lines of communication and modelling good digital behaviour. The right way of using parental control tools must be used to block harmful content, limit screen time, and monitor their children's online interactions. Parents must teach their children to adjust privacy settings to protect their personal information to reduce online crimes. Furthermore, parents must learn to educate their children about online safety like teaching how to behave respectfully online, educate their children about common online threats and predators, and explain the threat of sharing personal information, photos, or videos online. They must set clear instructions regarding screen time, social media use, and use of the internet. Most importantly, parents must create an atmosphere with their children in such a way that can foster trust among themselves. This will encourage honest communication and prevent cyberbullying or suspicious activities. Parents shouldn't fear reporting any cybercrime incidents to either schools, law enforcement, or appropriate authorities.

Therefore, their respective roles can help prevent cybercrime against children by offering education, supervision, and the right technological tools.

PSYCHOLOGICAL IMPACT ON CHILDREN

Numerous types of cyber-crimes against children including cyberbullying, online grooming, exploitation, and exposure to harmful content can result in intense psychological impacts. Children below the age of eighteen experience feelings of fear, shame, and helplessness, leading to anxiety, depression, and social withdrawal especially because minors are innocent, emotional and sensitive.

Children are most of the time targeted due to humiliation and isolation where harmful messages or images can be shared widely and permanently. Activities like online exploitation involving child pornography can extremely affect a child's self-esteem leading towards trauma, trust issues, and long-term emotional scars. These psychological impacts can affect a child's academic performance, relationships, and normal developmental milestones, requiring professional counselling and family support to help children process the emotional damage and recover their sense of safety.

CHALLENGES IN LAW ENFORCEMENT

The legal system comes across many challenges while focusing on cyber crimes against children. Firstly, jurisdictional complexity is one of the most prominent obstacles because cyber-crimes commonly cross national borders wherein it is difficult to determine applicable laws or to coordinate with international investigations. There are complications in tracking and identifying online predators due to the features provided by the internet. Digital shreds of evidence are temporary as they can be deleted or edited easily which makes it impossible to punish the offenders. Moreover, limited resources and technical expertise within law enforcement agencies further hinder their ability to stay ahead of constantly evolving cyber threats. Lack of specialized tools or training vital to confront cybercriminals and delays in adapting to new technologies allow offenders to exploit gaps in execution. There is an increasing need for public-private sector collaboration because private tech companies control most of the data needed for investigations. Altogether, these challenges create substantial barriers to effectively fighting cyber-crimes against children.

RECOMMENDATIONS FOR FUTURE ACTION

Several key actions must be taken to protect children from cyber-crimes effectively. International cooperation should be strengthened to handle jurisdictional challenges and improve the prosecution of offenders. Technological solutions, including advanced parental controls, AI-based monitoring systems, and encryption techniques should be stronger and implemented worldwide to discover and prevent harmful activities online. Schools must introduce detailed cyber safety education into their syllabus where both students and teachers are guided accordingly. In addition to that, parents also must receive guidance on how to foster safe online habits at home. There must be stronger enforcement of existing laws with necessary amendments and updating legislation to address emerging dangers and close any legal loopholes. Law enforcement agencies must be provided with sufficient training and resources to effectively combat cyber-crimes, while working closely with the private sector, particularly tech companies, to track and remove harmful content. Increased psychological support and counselling should be available to children who fall victim to cyber crimes, as the emotional toll can be significant. Developing specialized recovery programs will help ensure that these children can regain their mental and emotional well-being after such traumatic experiences. Implementing these recommendations is crucial because reports say that 445 crimes take place in a day which means 18 incidents per hour.

CONCLUSION

Cybercrime against vulnerable groups especially children is an increasing and concerning issue. Children are subjected to various threats in the digital world due to activities like cyberbullying and online exploitation. There is a need for rigid and strict improvement and innovation in fighting these crimes because protection from legal frameworks, technological tools, and educational programs contain loopholes. Every sector such as government, legal systems, private bodies, schools, parents, etc must come together, and collaborate to ensure the safety of children in cyberspace.

*****

UN CONVENTION ON CYBERCRIME: THE CONCEPT, CONCERNS AND NEGOTIATIONS

Sneha M.[80] and Pooja Shree[81]

ABSTRACT

Is the new draft of the United Nations Convention on Cybercrime an advancement in policy or diplomacy? This paper aims to answer the same. The rapidly evolving cyber threat landscape necessitates robust international cooperation, prompting the development of the UN Convention on Cybercrime. This landmark agreement aims to harmonize national laws, enhance international cooperation, and safeguard human rights in the face of escalating cyber threats. However, its implications for global cybersecurity governance warrant critical examination.

This study provides an in-depth analysis of the UN Convention on Cybercrime, focusing on the interplay between cybersecurity, human rights, and state sovereignty. A comprehensive review of the Convention's provisions reveals both strengths and weaknesses. On one hand, the Convention addresses emerging cyber threats, promotes international cooperation, and establishes guidelines for cybersecurity governance. On the other hand, concerns persist regarding human rights protections, the effectiveness of international cooperation mechanisms, and the Convention's adaptability to technological advancements.

The research investigates key questions inclusive of,

1. *Human Rights Protections: How effectively does the Convention balance cybersecurity concerns with human rights safeguards?*
2. *International Cooperation: What mechanisms does the Convention establish for inter-state cooperation, and how can they be improved?*
3. *Technological Adaptability: How well does the Convention accommodate emerging technologies and evolving cyber threats?*
4. *State Sovereignty: How does the Convention navigate tensions between national sovereignty and global cybersecurity governance?*

The findings contribute to the ongoing discourse on cybersecurity governance, informing policymakers, scholars, and stakeholders. This research aims to:

1. *Inform policy decisions on cybersecurity governance and human rights protections.*
2. *Enhance understanding of international cooperation mechanisms in cybersecurity.*
3. *Foster dialogue on the Convention's limitations and potential revisions.*

By examining the UN Convention on Cybercrime through a critical lens, this study sheds light on the complexities of cybersecurity governance and offers recommendations for addressing the challenges ahead.

INTRODUCTION

Cybercrime has emerged as a pervasive and insidious threat to modern society, the exponential growth of the internet and interconnected technologies has created vast opportunities for malicious

[80] Student at KLE Society's Law College, India.
[81] Student at KLE Society's Law College, India.

actors to exploit vulnerabilities, steal sensitive information, and disrupt critical infrastructure.

The far-reaching consequences of cybercrime transcend national borders, affecting individuals, businesses, governments, and entire economies. From identity theft and financial fraud to ransomware attacks and cyber espionage, the scope and complexity of cybercrime have escalated dramatically.

As the digital revolution continues to reshape the global landscape, the need for effective cybersecurity measures and international cooperation has become imperative. The UN Convention on Cybercrime attempts to address its global impacts, and the imperative for collective action to combat this burgeoning threat.

THE BUDAPEST CONVENTION

The first multilateral instrument to attempt global cybercrime regulation would be The Europe-led Budapest Convention, an international treaty focused on harmonizing national laws, and improving investigative techniques.

India is not a signatory to this convention, as it was negotiated and drafted without its participation, another primary contributor towards India's disinterest in the Budapest Convention would be, according to the Intelligence Bureau (IB), India, exchanging data with foreign law enforcement agencies would violate India's national sovereignty.

More prospective signatories opted out with the primary concern stemming from the limited involvement in its drafting process, leading to reservations about ratifying the treaty. India, for instance, has opted out, citing a lack of participation in its creation.

Another significant obstacle is the perceived threat to national sovereignty. Russia, among others, had expressed opposition, arguing that the Convention would undermine their autonomy and compromise law enforcement cooperation.

Major drawbacks of the Budapest Convention would be that it reflected Eurocentric focus, it faced negations from Russia and China as it was perceived to overstep national sovereignty of the party states, this would also be a primary cause for the lack of interest in the instrument.

The Budapest Convention also faced criticism due to the lack of safeguards provided for privacy and freedom of expression in varied regimes, and thusly didn't attract more signatories, it lacked universal adoption and thus failed at garnering global cooperation, the convention remained lost on the world with minimal impact.

UNITED NATIONS CONVENTION AGAINST CYBERCRIME

India is reconsidering its stance on a global instrument dealing with cybercrime since 2018 due to the surge in cybercrime.

India voted in favor of a separate convention under a Russian-led UN Convention against cybercrime (henceforth 'UNCAC') that would offer more measures on the ever evolving nature of the issue, with safeguards to the sovereignty of the party states. The then proposed convention received substantial push back from America and likeminded states, civil societies, and human rights institutions across the

globe, here the issues raised were that, with broad powers vested in legislations, it opens up more avenues for regimes to prosecute dissent and activism, and allows massive rampant surveillance, violating privacy.

The UNCAC is the second such global effort at cybercrime regulation, the deliberations towards this 41 paged document lasted over three years with the title being settled mere weeks before the adoption by the UN ad-hoc Committee (henceforth 'UNAHC').

The Deliberations for this global instrument lasted over three years, throughout which different countries moved motions in support of their national needs and agendas. An analysis of the said deliberations would provide us with insights into the future implications of the UNCAC in different nations.

Developing countries stressed the need for capacity-building and technical assistance to bridge cybersecurity gaps, thus, Article 1(c) from the statement of purpose pledges resources towards developing countries to ensure harmonious global co-operation in tackling all the facets of cybercrime, this move is seen necessary from the global community as the weak policies and enforcement mechanism in developing countries shelters the sources of cybercrime.

Article 1(c) also makes an effort to move away from the criticism of euro-centrism of its predecessor, potentially attracting more developing countries for signatories to bridge the gap that the Budapest Convention left. This addition could potentially save the move from failing.

Article 5 of the same document addresses the impact on sovereignty of the party states addressing the concerns and reassuring the sovereignty of the party states, so Article 1(c) and 5 seems to address the primary flags that were raised against the adoption of the Budapest Convention.

Article 6 - "Respect for human rights" adds directions for the state legislations towards compliance with Human Rights, the provision comes after much insistence by numerous civil societies and human rights institutions.

The draft United Nations convention against cybercrime draws the core resolutions against cybercrime from the Budapest Convention on Cybercrime, 2001, it also includes provisions adapted from the UN conventions on Transnational Organised Crime, 2000 and Corruption, 2003. But it is interesting to note here that the new draft does not include the advanced tools that are employed in the 2nd protocol to the Budapest Convention that would be critical for enhanced cooperation and disclosure of electronic evidence.

Inclusion from the Budapest Convention establishes the relevance of the document in today's landscape of cybercrime, and might reduce the present draft to a mere diplomatic advancement, as Australia and likeminded states were throughout of the opinion that the Budapest convention, already in place, addresses cybercrime offences, jurisdiction and international co-operation along with establishing procedural law, mutual assistance and extradition sufficiently.

DELIBERATIONS

The UN convention on cybercrime is the first legally binding global instrument to tackle cybercrime,

as it involves a complex, open ended ad hoc committee process, the deliberations saw participation from developing countries, making it a more inclusive and widely acceptable instrument, something that the Budapest Convention had failed to do with its 76 signatories, it was thusly was much criticized for excluding the developing countries during its deliberations. The UN convention on the other hand is expected to bridge the gaps in the global map that were left by the Budapest Convention, this would implicate a greater possibility of the convention being more successful in achieving its objectives.

The UN Conference on Cybersecurity convened with 70 speakers sharing insights on threats, national experiences, and the Security Council's role in addressing cybersecurity concerns. UN Secretary-General António Guterres stressed the importance of leveraging digital breakthroughs for global betterment, emphasizing conflict prevention and cybersecurity, leading the deliberations. The conference highlighted the alarming integration of digital tools with weapons systems, creating vulnerabilities, and the growing use of AI in cyberoperations. Another area of concern and deliberation was ransomware surge, as ransomware payments skyrocketed to $1.1 billion in 2023, compromising public institutions, electoral processes, and online integrity.

The conference emphasizes global cooperation, as Speakers underscored the need for international collaboration to combat cyber threats, acknowledging resource gaps in many countries, as reflected in the third statement of purpose.

During the deliberations of the UNCAC, nations adopted diverse stances and made substantial contributions. Delegations from different countries put forth motions in advancement of their national concerns and agendas,

The UNCAC has sparked a global debate, reflecting the complex and often conflicting interests of various countries regarding how to regulate and combat cybercrime. These discussions are part of an ongoing international effort to establish a comprehensive legal framework for addressing the rapidly growing threat of cybercrime, which has evolved with the expansion of digital technologies. However, the participating nations are “poles apart” on many critical issues, such as the scope of the treaty, the balance between security and human rights, and the implications for state sovereignty and internet freedom.

The primary divide in the negotiation’s centers on two competing visions for the treaty: one focused on combating specific criminal activities in cyberspace and another that seeks to extend the treaty’s scope to include broader control over digital content and information.

On one side, Western nations, including the United States, members of the European Union, and several other democracies, advocate for a narrow and targeted treaty. These countries want the treaty to concentrate on addressing defined cybercrimes such as hacking, ransomware attacks, identity theft, and fraud. They emphasized the importance of ensuring that the treaty does not infringe on human rights, particularly the rights to privacy, free expression, and access to information. Many Western countries are also concerned about the potential for the treaty to be used as a tool for state surveillance or to justify repressive measures, especially in authoritarian regimes.

For instance, the European Union pushed for language in the treaty that would explicitly protect individual privacy rights and guarantee that any law enforcement cooperation in cybercrime investigations adheres to established human rights standards. The EU's concern is that a poorly defined or overly broad treaty could undermine the fundamental freedoms that underpin democratic governance and the open nature of the internet.

On the other side, Russia, China, and some other authoritarian-leaning states advocate for a broader interpretation of cybercrime that includes regulations on online content, misinformation, and other forms of digital communication. Their stance reflects a desire to exercise greater control over the internet within their own borders, using cybercrime as a justification for increasing state regulation and censorship of digital spaces. For these countries, issues like disinformation, online extremism, and political dissent are seen as threats that can and should be controlled through legal means.

Russia has been a particularly vocal proponent of this approach, suggesting that the treaty should not only target cybercriminals but also regulate content that undermines state authority or spreads harmful information. This position has led to significant criticism from human rights groups, who warn that such provisions could enable states to crack down on legitimate political dissent or restrict the free flow of information online.

The positions of developing countries further complicate the negotiations. Many developing nations are concerned about their limited capacity to deal with cybercrime, as they often lack the technical resources and expertise to combat sophisticated cyber threats. As a result, these countries have called for greater international cooperation, capacity building, and resource sharing as part of the treaty. They seek assurances that wealthier nations will provide the necessary support to help them address cybercrime effectively.

At the same time, some developing countries also support broader provisions that would give states more control over digital content, reflecting concerns about the destabilizing impact of misinformation, especially in fragile political environments.

For these countries, cybercrime is not just about financial theft or data breaches but also about the potential for digital platforms to undermine governance and social stability.

The negotiations are at a delicate juncture, with wide-ranging views on what the final treaty should look like. Finding a balance between security and freedom is the central challenge. Many observers worry that without careful safeguards, the treaty could be used to justify overreach by authoritarian governments, while others are concerned that too narrow a focus might leave significant cyber threats unaddressed.

Despite the divide, there is broad agreement that international cooperation is essential in tackling cybercrime. Cyber threats are global, and no country can effectively address them in isolation. However, the path to a treaty that satisfies the concerns of all parties remains fraught, with countries continuing to be "poles apart" on key issues. The outcome of these negotiations will shape the future of international cybersecurity policy and the balance between state security and individual freedoms in the digital age.

During the deliberations on the provisions of human rights, India backed Iran's proposal to delete clauses allowing states to refuse personal data requests that may lead to prosecution based on political views, race, or ethnicity.

Furthermore, India, alongside 22 other nations, voted to eliminate Article 6(2), a vital human rights safeguard. This clause ensured that the convention wouldn't be used to suppress fundamental freedoms, though the Iran's proposal failed to have its motion passed the convention lacks robust human rights protections, assuming countries will act in good faith. This assumption is flawed given the diverse human rights standards globally.

The delegation from South Korea urged for a strengthened security council engagement to counter cyber threats, citing North Korea's sanctions evasion through digital means.

Ukraine put forth a plea against Russia's cyber aggression, including sophisticated attacks on government, security agencies, businesses, and critical infrastructure.

Russia, Belarus, China, Nicaragua, and Cuba, in consensus proposed expansive criminalization of cyber-enabled crimes, including content-based offenses like inciting subversion or armed activities and ICT-facilitated coercion.

Russia has taken a robust stance on the UN Convention on Cybersecurity, advocating for an expansive definition of cybercrime. This includes content-based offenses such as inciting subversion or armed activities and ICT-facilitated coercion, sparking concerns among Western officials and human rights groups.

They worry that Russia's approach could legitimize authoritarian digital sovereignty models, undermining online freedoms. In 2019, Russia, China, Iran, and North Korea supported a UN General Assembly resolution aimed at establishing an international convention to counter criminal uses of ICTs.

Critics argue that Russia's efforts aim to shift global cyber norms toward authoritarianism, potentially criminalizing free expression and circumventing humanitarian law obligations.

Chile, Canada, and the UK, these countries championed integrating a gender perspective into the treaty, acknowledging unique cybersecurity risks and experiences across genders.

EU member states, the US, the UK, Japan, and Australia, these nations advocated for a focused approach, targeting core cyber-dependent crimes and select cyber-enabled crimes, such as child exploitation.

Key Concerns of the UNCAC would be the threat it poses to free speech, dissent and activism through Surveillance Expansion, Russia's proposal may justify increased state surveillance and censorship.

It could hinder free speech further in authoritarian regimes, as it would restrict expression due to availability of provisions to prosecute the same, the broad cybercrime definition could limit online freedom of expression, thus hindering digital sovereignty, Russia's push may undermine global human rights and democracy promotion online.

The United States has taken an active role in discussions on cybersecurity at the United Nations, with a focus on establishing a safe, open, and interoperable cyberspace. During deliberations at various UN conventions, the U.S. has consistently pushed for certain key proposals and policies, aimed at shaping international cybersecurity governance.

The U.S. strongly advocated for the application of existing international law to cyberspace, particularly the principles laid out in the United Nations Charter. During UN discussions such as those led by the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG), the U.S. has argued that international law, including state sovereignty and non-interference, must extend to cyber operations. This includes a clear prohibition on the use of force or interference in domestic matters via cyber activities.

One of the primary U.S. proposals is the promotion of confidence-building measures (CBMs) to reduce cyber-related risks between states. These measures, which include increased transparency, information sharing, and the creation of communication channels between nations, aim to prevent misunderstandings and potential conflicts that could arise from cyber incidents.

In terms of combating cybercrime, the U.S. supports the use of existing international legal frameworks, particularly the Budapest Convention on Cybercrime, which provides a comprehensive international legal standard for addressing cybercriminal activities. The U.S. opposes efforts to create new, potentially conflicting frameworks, as proposed by some countries like Russia and China, which could undermine current efforts and restrict digital freedoms.

The U.S. has consistently voiced its opposition to proposals supporting cyber sovereignty, a model championed by countries such as Russia and China. These proposals argue for greater national control over cyberspace, allowing governments to restrict or monitor the internet within their borders. The U.S. opposes this vision, advocating instead for a global and open internet, which would preserve the free flow of information and protect freedom of expression.

The U.S. also emphasizes the importance of capacity building in developing countries, arguing that many nations lack the expertise and infrastructure to effectively counter cyber threats. The U.S. supports international cooperation in strengthening technical knowledge, improving cybersecurity infrastructure, and building frameworks to assist developing nations in securing their cyberspace.

The U.S. consistently links cybersecurity to the protection of human rights. It argues that cyber regulations should not infringe on fundamental rights such as privacy, freedom of expression, and access to information. The U.S. has repeatedly called out authoritarian regimes for using cybersecurity as a pretext for limiting internet freedoms and human rights.

In line with its broader internet governance philosophy, the U.S. supports a multi-stakeholder approach to cybersecurity, which includes contributions from not only governments but also the private sector, civil society, and academic institutions.

This model ensures a more open and collaborative approach to internet governance, in contrast to the state-controlled models advocated by countries like China and Russia.

Throughout various United Nations discussions, the U.S. has sought to balance the need for robust cybersecurity with the preservation of human rights and an open, global internet. It has consistently pushed for the application of international law to cyberspace, promoted collaboration and capacity building, and resisted efforts to impose more restrictive, state-centric internet governance models. The U.S. approach focuses on international norms, cooperation, and the protection of digital freedoms, often in opposition to authoritarian countries proposing stricter control over cyberspace.

IMPLICATIONS FOR INDIA

The UN Draft Convention's adoption will significantly impact India's cybercrime and cybersecurity legal framework, potentially requiring amendments to existing legislation (e.g., Information Technology Act, 2000) or enacting new laws.

India's Cybercrime Laws are dispersed across Information Technology Act (2000), CERT-IN Framework, Digital Personal Data Protection Act (2023), Criminal laws, and Sectoral regulations. The National Cyber Security Policy (2013) is currently in effect, with an updated strategy aligned with international standards anticipated.

Several human rights institutions expressed their discontent with the present draft that would empower different regimes against dissent and activism, their concerns revolved around the overly broad scope and definition potentially leading to misuse. The insufficient human rights safeguards, particularly freedom of expression and privacy, require strengthening.

The same institution has written to the UNCAC before the adoption of the draft addressing the same concerns and recommendations, primarily to establish clear, concise definitions of cybercrime and cyber-dependent crimes. To lean towards robust human rights protections and targeted capacity building and provide tailored technical assistance to address state capacity disparities.

The Knowmad Institut, an organization focused on human rights and drug policy, made several key recommendations to the United Nations convention on cybersecurity, emphasizing a balance between security, human rights, and digital freedoms. Their approach is centered on ensuring that cybersecurity frameworks respect fundamental freedoms, avoid excessive government control, and promote ethical use of technology.

1. Human Rights-Centered Approach

The Institut advocates for a cybersecurity framework that prioritizes the protection of human rights, particularly freedom of speech, privacy, and access to information. They argue that cybersecurity measures should not become tools for government surveillance or the suppression of dissent.

The Knowmad Institut warns against overregulation in cyberspace, which could lead to mass surveillance or the curbing of digital freedoms. They recommend that any international cybersecurity framework be designed to prevent states from infringing on individual privacy and digital rights under the guise of security measures.

2. Transparency and Accountability

The Institut stresses the importance of transparency in cybersecurity governance. They argue that any

cybersecurity policies developed at the UN level should ensure that states are held accountable for their actions in cyberspace, particularly in the use of surveillance technologies.

3. Promotion of Ethical Technology Development

The Institut recommends promoting the development and use of technology that is ethical and respects human rights. They suggest that cybersecurity efforts should not only focus on defending against cyberattacks but also consider the long-term societal impacts of technological innovations.

4. Collaboration Across Sectors

The Institut emphasizes the need for a multi-stakeholder approach, bringing together governments, civil society, the private sector, and technical experts to create a comprehensive and inclusive cybersecurity framework. This approach would ensure that diverse perspectives are considered, reducing the risk of authoritarian policies being adopted.

In summary, the Knowmad Institut's recommendations to the UN on cybersecurity call for a balanced approach that protects security while safeguarding human rights, promoting ethical technology, and ensuring transparency in governance.

*****

MACHINE LEARNING AND PREDICTIVE ANALYTICS AS MEANS OF SAFEGUARDS WITH SPECIFIC REFERENCE TO ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY RIGHTS

Dr Lisha Azeez[82]

ABSTRACT

Salesforce software is the main widespread Artificial Intelligence for Customer Relationship Management (CRM). It is a combined set of Artificial Intelligence technology that creates Salesforce Customer more effective and acquires Artificial Intelligence all over the place. Software is readily incorporated into numerous Salesforce products and no need to do formulate several facts and data or handle several replicas. Fundamentally placing material/statistics in Salesforce and structures mechanised by software will apply to enable data in to more efficient and analytical method regarding the customers. Software is available all over Sales Cloud, Service Cloud, Marketing Cloud, App Cloud, Analytics Cloud, and Community Cloud. The listed owner of the Software has the exclusive right to use the intellectual property rights involved in the software. If anybody misapplications the procedure of trademark or copyrighted works in the software, the concerned will be liable for equally civil and criminal actions as per the prevalent regional and international laws. Third parties are not permissible to use the trademark and copyrighted works of the software without previous authorization of the registered owner. Everyone will be responsible for vigilant assessment as an entire matter, while utilising Salesforce's trademarks or copyrighted works. The listed owner can modify or take out at any time, any approval to use trademarks and copyrighted works except specifically striped in an agreement. All rights permissible to use trademarks and copyrighted works entail that the trademarks and copyrighted works be appropriate to the registered owner, for circumventing problems related with ownership of Software and its trademarks and/or copyrighted works.

Keywords: Sales force; Software; Artificial Intelligence; Copyright; Trademark.

INTRODUCTION

Salesforce software is the main comprehensive Artificial Intelligence for Customer Relationship Management (CRM). It is a combined set of Artificial Intelligence technology that creates Salesforce Customer more effectual and becomes Artificial Intelligence all over the place. It is readily combined into numerous Salesforce products and no need to do make several facts and data or grip several reproductions. Basically placing material/statistics in Salesforce and structured mechanisms will utilize to enable data in to more well-organized and logical manner regarding the customers. It is easy to get to throughout Sales Cloud, Marketing Cloud, Analytics Cloud, and Community Cloud.

- Data — Easily fortified with data after inclusion in the Salesforce. It will work out the data precisely. So it is time saving and no need to provision of data and statistics in physical mode. Hence it is easy to cope.
- Machine Learning Tools — Computerized mechanism affords the detailed and accurate reproduction regularly without any human involvement and also identify the indispensable data to the organization.

[82] Associate Professor in Law cum Vice Principal, Nehru Academy of Law, India.

- Result — Absolute and precise results will be there. It is a component of the indistinguishable and consistent Salesforce policy, with appropriate supervision and examining of meticulous tools for better results.
- Sales can forecast further probabilities and also requirements and inevitabilities of consumers.
- Service can be applied by decisive cases prior to happen
- Marketing can generate logical expedition with an remark like never earlier
- IT can drive in capability all over the place and form apps for human resources and users

Role of Intellectual Property :-

It comprises:-

a. website content
b. brand names
c. videos
d. logos
e. other material protected under trademark or copyright law.

LEGAL ANALYSIS

The Incorporation of any portion of trademarks or symbol or any other distinguishable fragment in Software's name, app name, website name, domain name, social media or any other categorizing materials as others realm /website address is not permissible exclusive of preceding inscribed authorization, or through an agreement. It is not practicable to use any part of trademark associated with the software that is to be perplexed with any part of software's well-designed areas. The transformation such as foreign language summary of any of part of software and purchase of any component of the trademark with respect to software for promotional actions are not allowed without approval. Demonstration or make use of any part of logo, designs, website content, videos, testing materials, and alteration or change or any other trademark or copyrighted work of Software as their actual for marketing policy in any process are not permissible. The outline and extents used for the software, disingenuous others and using of the source code and machine languages, programs used in the software are against the fundamental Laws. The right to progress the software without prior authorization of the registered owner will fascinate the infringement as per legal provisions.

The registered owner of the Software has the special right to use the intellectual property rights comprised in the software. If anybody misapplications the practice of trademark or copyrighted works in the software, the concerned will be liable for both civil and criminal actions as per the prevalent regional and international laws. Third parties are not permissible to use the trademark and copyrighted works of the software without prior authorization of the registered owner. Everybody will be accountable for vigilant valuation as a whole while utilising Salesforce's trademarks or copyrighted works. The registered owner can modify or take out at any time, any approval to usage of trademarks

and copyrighted works excluding specifically striped in an agreement. All rights permissible to use trademarks and copyrighted works necessitate that the trademarks and copyrighted works fit to the registered owner, for circumventing problems linked with ownership of Software and its trademarks and/or copyrighted works. No assurance of any arrangement with any approvals will be assumed to anybody connected with trademarks and copyrighted works. No relocation is applicable associated with the rights previously approved to anybody else. The practice of any portion of trademarks of software is aggressive except written authorization in an agreement or supplementary action, or by making perfect a permissible use . After granting of the approval also, the owner have the right to modify or rescind permission , save as otherwise striped in an agreement.

Software retain copyright in its website, logos, designs and content, videos and further persuasive materials, and its proprietary computer code, as well as any further machine languages and codes etc. So not realistic to abuse, replicate, dispense, or create derived works from any copyrighted work, or any serving of a copyrighted work, owned by the owner of the software exclusive of accomplishment to an authorization or a comprehensive consensus with an agreement to Use Trademark and/or Copyrighted Work form linked with the software. The exercise to shorten any part of trademarks related with the software in modified arrangement is repugnant. The owner of a copyright has the right to forbid others from copying, distributing, generating unoriginal works or or else by means of the limited precise.

Trademark guarantees consumers of consistent worth with regard to those merchandise or services and assistances in the advertising too. Hence if anyone infringes too, it will affect the reputation and goodwill of the organization. Trademarks in manifestation form only to demonstrate properly how the services correlated with the software will work out. This software appliance will work on mobile device. More than 150,000 companies are expending this software all over the world. It is very adaptable and consistent in nature and will get entry on data with more nonviolent and protected. It is a great setting up to the organization and shows a dynamic character too. The organizations can diminish the human resources and use this software for immediate communications without any obstructions. They can evaluate about the requirements, needs and taste of consumers and mandate in the market policies. It also enables to forecast the oppositions too. It also affords material and the current status of the innovative techniques and improvement in the business related activities. It also provides appropriate resolutions on time by taking conclusions on time. It is an advanced method to get easy factual of entry about the substantial by scanning company's logo in no time. It simplifies to measure the choices of customers in all networks. It offers information in depth about the consumer satisfaction and suitable decision constructing process too. It will upsurge the effectiveness of managerial techniques and approaches. It will develop the fitness of the group and its future too. Anyone can use this software in a simple way and implement it fastly for smooth consecutively of the organization. It seems like a new Business Intelligence or analytics tool looming out each time.

PROTECTION OF IPRS VIS A VIS ARTIFICIAL INTELLIGENCE

A suggestion for registration of a trademark should be trooped with the suitable countrywide or provincial Trademark Office. The claim should include a understandable replica of the indication filed for registration as well as any insignia, forma or three-dimensional nature. The request must also enfold

a catalog of commodities or amenities to which the suggestion should be pertinent. For a mark to get arranged it should comprehensive to two conditions.

Primary, the mark must be eccentric, so that customers be talented of distinguish it from extra trademarks and products.

Next, the mark should not be viewed with distrust. It means the mark be imaginary to not mislead, be disloyal to the consumers or infringe community command or ideologies. For this purpose, it is good to select a mark, which is unassuming to utter, keep in mind, include and be familiar with. The most exceptional trademarks are the brand something own words or made-up lexicon. Avoid terminology languages for the mark. Favoring physical name representing the source of the commodities and flattering vocabulary which elucidate the renown of the commodities such as unmatched, faultless, quality etc. as create name is also inappropriate. The vessel of the mark is capable to file acquiescence for trademark registration.

Trade Marks Act 1999 make available protection to the owner of the mark to make sure controlled right to make usage of it, to distinguish the merchandise or services or to give authorization others to use it in return for fee. Trademark security is mandatory by which in most assembly have the ability to obstruct trademark violation. It promotes resourcefulness and undertaking wide-reaching by sustaining the owners of Trademarks with identification and economic continues. It also hinders the efforts of unnecessary applicants such as imitators to make use of related distinctive symbols to open market subnormal or assorted products or services. It is a mixture of terminology, inscription and form. It possibly will entail of illustration, cryptogram, three- dimensional symbols such as the nature and wrapping of produce, adept of being heard cipher such as arrangement or choral resonance, fragrance or ensign used as distinguishing features.

Trademark can be listed even in the person's name, corporation or organization, which be able to signify by its owner or traitor or executive as the case may be. No individual shall be permissible to present any incidence to stop or to get improved compensation for the infringement of an unregistered trademark. Only the owner of a registered trademark be capable to use the representation ® in India. By means of the sign ® excluding the mark has been registered is unlawful in India. Using mark TM with trademark simply way that one preserve to be the owner of the trademark. There is no ban to create use of of the pictogram TM in India. The expression of protection of trademark shall be in the beginning for a period of 10 years. It can be transformed for an unlimited period each ten years by giving the renewal fee.

CONCLUSION

In view of the above, it is obvious that Salesforce plays a dynamic role for prompt entree of data and also enables to take timely conclusions and alternate resolutions as per the enlightened marketing strategies. Moreover, the Artificial Intelligence and Intellectual Property Rights such a trademark and copyright also show an imperative part and no one is permissible to use the IP rights without the authorization of the registered owner. If anybody invades the same, the concerned will be disciplined as per the foremost Regional and International Laws.

*****

REFERENCES

1. WIPO Handbook
2. Trademarks Act 1999
3. Copyright Act 1957
4. George Luger, Artificial Intelligence : Structures and Strategies for complex problem solving, fourth edition – Addison Wesley, 2002 – introduction to artificial intelligence http://www.aaai.org/AITopics

*****

A GLANCE AT THE ROLE OF POLICE IN COMBATING CYBER CRIME WITHIN THE LEGAL FRAMEWORK OF INDIA

Jaswant Singh[83] and Dr Haider Ali[84]

ABSTRACT

The rise of cybercrime has fundamentally altered our understanding of the term "space" in relation to crime. We can no longer view crime and criminality solely through a geographical lens. Cybercrime defies traditional borders, often extending beyond physical limitations. While advancements in Information and Communication Technology (ICT) have greatly benefited society, they have also facilitated a variety of illicit activities conducted online, such as hacking, identity theft, online fraud, cyberbullying, & cyber terrorism. These activities present significant challenges, as they utilize sophisticated technological tools to exploit vulnerabilities. In India, the widespread availability of internet access and the rapid digitization of services have made the nation particularly appealing to cybercriminals, who take advantage of weaknesses in networks, systems, and the naivety of users. As one of the world's largest and fastest-growing digital economies, India is especially at risk from cyber terrorism. Consequently, cybercrime is increasingly recognized as a major societal challenge, prompting a critical need for governments to take decisive action. In response, various legislative measures and institutional frameworks have been established to tackle the complexities of the cyber realm. Nonetheless, due to the ever-evolving nature of cyberspace, there is an urgent need for enhanced cyber policing and thorough investigations into cybercrime. The primary aims of my research paper are to explore how police can be effectively regulated in their efforts to combat cybercrime, to gain insights into the nature of cyber policing and its inherent challenges, to examine theoretical models of cyber-crime investigation, and to discuss various issues and obstacles faced in cyber policing & cyber-crime investigation.

Keywords: Transcending, Geographical, Boundaries, Mechanism, Information and Communication Technology

INTRODUCTION

The emergence of cybercrime has fundamentally altered the concept of ‘space’ within the realm of criminal activity. We can no longer limit our understanding of crime to geographical parameters; instead, cybercrime operates beyond physical borders, defying traditional definitions. While advancements in ICT have brought numerous benefits to society, they have also facilitated a spectrum of illicit activities conducted online, such as hacking, identity theft, online fraud, cyberbullying, & cyber terrorism. These developments present both significant challenges and opportunities, as they employ sophisticated technological tools for criminal purposes.

The widespread availability of internet access and the swift digitization of services have made India an appealing target for cybercriminals, who take advantage of vulnerabilities in networks, systems, and unsuspecting individuals. As one of the largest and fastest-growing digital economies globally, India is particularly susceptible to threats from cyber terrorism. Consequently, there is an increasing recognition of cybercrime as a major societal issue, highlighting the urgent need for governments to respond effectively. In response, many governments have enacted legislation and set up institutional frameworks to tackle the complexities of the cyber landscape. Nevertheless, given the rapidly evolving nature of

[83] Research Scholar at Institute of Legal Stdies and Research, Mangalayatan University, Aligarh, India.
[84] Assistant Professor at Institute of Legal Stdies and Research, Mangalayatan University, Aligarh, India

cyberspace, there remains an urgent need for enhanced cyber policing and more robust investigations into cybercrime.[85]

NATURE OF CYBER POLICING

When cyber-crimes occur, law enforcement agencies bear the responsibility of investigating these incidents and apprehending those responsible. This responsibility often falls to specialized cyber-crime units within police departments, commonly referred to as cyber police.[86]

Key considerations regarding cyber policing include:

- What defines the role of cyber policing?
- Can public law enforcement effectively address the challenges posed by cyber-crime on its own?
- Is it feasible for cyber policing to manage these threats independently?
- Should private corporations or non-governmental organizations (NGOs) be involved to achieve more effective outcomes?

The IT Act aims to provide answers to these questions by establishing a legislative framework for cyber policing in India through its various provisions. For instance, Section 69[87] empowers the government or designated agencies to intercept, monitor, or decrypt information generated, transmitted, received, or stored within computer resources, provided that procedures outlined in the section are followed. This authority can be exercised if Central or State Government determines it is necessary to protect sovereignty & integrity of India, national defense, state security, friendly relations with foreign nations, public order, or to prevent incitement to any cognizable offense related to these areas or for the investigation of any crime.

In such instances, prescribed procedures must be adhered to, and the rationale for such actions must be documented by the appropriate government agency. Additionally, intermediaries are required to provide technical assistance and facilities when requested. This assistance can include:

- Granting access to computer resources containing relevant information.
- Facilitating the interception, monitoring, or decryption of information as necessary.
- Supplying information stored in computer resources.

Failure to comply with these requirements can result in imprisonment for up to seven years and the imposition of fines.

Section 69A of IT Act, 2000,[88] gives Central Government or its officials authority to block public access to certain information via computer resources. Meanwhile, Section 69B discusses power to authorize monitoring & collection of traffic data through computer resources to bolster cybersecurity. Central

[85] Charles Chatterjee & Anna Lefcovitch, *Cyber Security, Diplomacy and International Law*, 108 AMICUS CURIAE 2 (2016).
[86] Emeka C. Adibe, Ndubuisi Nwafor & Chibuike Amaucheazi, *Information Technology, Terrorism Financing and Financial Institution's Role in Combating Terrorism*, 2 IRLJ 29 (May 2020).
[87] Information Technology Act, 2000, § 69 (2000).
[88] Information Technology Act, No. 21 of 2000, § 69A (2000).

Government can notify any government agency to collect traffic data generated, transmitted, received, or stored within computer resources, aiming to enhance cyber security & to identify, analyze, and prevent the spread of intrusions or computer viruses within country.

Traditionally, responsibility for monitoring the cyber landscape has been viewed as falling solely to public law enforcement. However, academic discussions suggest that monitoring can also be effectively carried out by corporate security forces and NGOs. The effectiveness of cyber policing will hinge on fostering collaboration among public police, corporate entities, and non-governmental organizations. The task of policing cyberspace is becoming increasingly challenging due to the high mobility of cyber criminals.

COORDINATION/INTERNATIONAL PROTOCOLS AMONG COUNTRIES

Criminal investigations in cyberspace present unique challenges that differ significantly from those in the physical world. The virtual environment eliminates traditional barriers, fosters anonymity, and creates geographical detachment, which necessitates a reevaluation of crime and its perpetrators. In this digital realm, a criminal and their victim may exist in entirely different locations, often lacking any direct connection. Consequently, investigative processes must navigate not only the laws of individual states but, in some instances, the legal frameworks of multiple countries. This complexity underscores the need for enhanced understanding, collaboration, and coordination among legal authorities across various jurisdictions.

To address these challenges on an international scale, Budapest Convention on Cybercrime was established as first treaty aimed at tackling internet & computer-related offenses.[89] This convention seeks to harmonize national laws, improve investigative methodologies, and foster greater cooperation between nations. It officially took effect on July 1, 2004. However, the convention has yet to gain widespread acceptance, with several countries, including India, opting not to ratify it due to concerns over national sovereignty and its absence from initial drafts.

CYBER CRIME INVESTIGATION

Cybercrime units are tasked with investigating incidents of cybercrime and apprehending those responsible. They utilize specialized teams equipped with advanced skills and technologies to gather evidence, trace digital activities, and initiate legal proceedings. O Ciarduain identifies a framework known as the 'Extended Model of Cybercrime Investigation,'[90] which includes thirteen critical activities outlined below:

- Awareness – recognizing the need for an investigation.
- Authorisation – acquiring legal permission, such as a warrant.
- Planning – utilizing the information collected by investigator.
- Notification – alerting subjects & relevant parties that investigation is underway.

[89] European Treaty Series - No. 185, Convention on Cybercrime, Nov. 23, 2001.
[90] Ó Ciardhuáin, Séamus. "An Extended Model of Cybercrime Investigations." *International Journal of Digital Evidence* 3 (2004).

- Search & Identification of Evidence – locating devices, such as computers used by suspects.
- Collection of Evidence – securing potential evidence for further examination.
- Transportation of Evidence – moving evidence to designated location for analysis.
- Storage of Evidence – ensuring that storage practices minimize the risk of contamination.
- Examination of Evidence – employing specialized techniques to recover deleted data.
- Hypothesis – developing a provisional explanation of the events.
- Presentation of the Hypothesis – communicating findings to a jury or other relevant parties.
- Proof/Defense of the Hypothesis – considering alternative explanations and counterarguments.
- Dissemination of Information – sharing insights that may inform future investigations.

Understanding the cybercrime investigation process in India is essential for this module. According to Sec. 78 of Act, 2008,[91] authority to investigate cybercrimes is specified, stating, "Notwithstanding anything contained in Cr.P.C., 1973, no police officer below rank of Inspector shall investigate any offence."

Sec. 80 grants police officers & authorized personnel the power to enter and search premises without a warrant. It specifies that officers of a certain rank may apprehend individuals reasonably suspected of committing, attempting to commit, or being in act of committing an offence. Furthermore, Sec. 80(2) states that if a person is arrested by officer other than police officer, they must be presented before Magistrate or officer in charge of police station without unnecessary delay.

The challenges faced in cybercrime investigations are primarily due to jurisdictional limitations, ambiguities in the law, and a lack of understanding of technology-based crimes among key stakeholders in the criminal justice system. Many states operate with only one or a handful of specialized cybercrime units, which are often overwhelmed by the rapid increase in cyber offenses. Victims frequently encounter difficulties in accessing the appropriate police stations to file their complaints. The major obstacles in cybercrime investigations include:

- A shortage of trained cyber investigators.
- Limited availability of cyber forensic facilities in forensic laboratories.
- Delays in obtaining forensic reports due to significant backlogs.
- Insufficient institutional mechanisms for accessing expertise from the cyber industry.

The effectiveness of law enforcement in cyber policing and investigation fundamentally hinges on the capacity of these units. The skill set of personnel assigned to cybercrime investigation units is crucial for operational success. Existing recruitment standards for police in India may not adequately address the unique demands of this field. Therefore, it is imperative for Indian law enforcement agencies to

[91] Information Technology (Amendment) Act, No. 10 of 2009, § 78 (India).

attract and employ top talent in cyber technology to effectively combat the evolving threats posed by sophisticated cybercriminals.

LEGAL FRAMEWORK OF CYBER LAW

Domain of cyber policing & cyber-crime investigation is characterized by rapidly evolving landscape, presenting numerous challenges that require attention. A primary concern within this realm is the legal framework governing cyber activities. In India, prior to implementation of IT Act, 2000, cyber landscape was largely unregulated, leading to considerable uncertainty among law enforcement regarding the handling of crimes committed online. The introduction of the IT Act marked a significant turning point, as it provided a legal foundation for defining cyber-crime and establishing procedures for cyber policing and investigations.[92]

Recognizing the need for adaptability in response to the dynamic nature of cyber-crime, amendments were made to the Act in 2008. These revisions expanded the scope of cyber-crimes to include offenses such as child pornography and cyber terrorism, while also shifting investigative authority from the Deputy Superintendent of Police to Inspectors. This evolution raises critical questions that the legal framework must address, including:

- What constitutes cyber-crime?
- What procedures are to be followed in investigating cyber-crimes?
- What penalties will apply to individuals convicted of such crimes?
- How is evidence defined within the context of cyberspace?

Effective legal frameworks are crucial for prosecuting cyber criminals and deterring potential offenders. In India, various laws, including the IT Act, 2000 and its subsequent amendments, have been enacted to tackle different facets of cyber-crime. The police play a vital role in enforcing these laws and delivering justice, working to ensure that the legal infrastructure is sufficient for the prosecution of cyber criminals. Notably, the IT (Amendment) Act, 2008, grants police officer's specific powers to investigate cyber-crimes, including the authority to conduct searches and make arrests without a warrant.

LANDMARK JUDGEMENT OF SUPREME COURT

In *Prakash Singh & Ors. v. Union of India & Ors.*,[93] court included a significant directive: it advocated for the separation of investigative police from those responsible for maintaining law and order. This separation aims to enhance the efficiency of investigations, improve expertise, and foster better relationships with the community. The need for cooperation between these two branches was also stressed. This principle has been reiterated in the Model Police Act, 2006, with several state legislatures adopting these recommendations verbatim.

[92] Scott J. Shackelford, *Inside the Drive for Cyber Peace: Unpacking Implications for Practitioners and Policymakers*, 21 U.C. DAVIS BUS. L.J. 285 (Spring 2021).
[93] Writ Petition (Civil) 310 of 1996.

The underlying implication is that law enforcement personnel require specialized training, particularly given the complexities of contemporary crime, including cybercrime, which necessitates advanced investigative skills. This calls for the recruitment and training of dedicated personnel to address these challenges effectively, ensuring they can develop their expertise over time. Additionally, it is noteworthy that court previously invalidated Section 66A, deeming it unconstitutional. This provision was criticized for being excessively restrictive and for leading to the detention of individuals for sharing content deemed objectionable.[94]

CONCLUSION

Contemporary landscape of cyberspace poses significant challenges for criminology, police science, law enforcement, & policing. In India, combating cybercrime has become a persistent challenge that necessitates a collaborative approach among law enforcement agencies, governmental entities, the private sector, and the general public. Since the 1990s, cyberspace has developed into a significant domain for criminal activities, fundamentally altering the nature and breadth of crime and victimization. This evolution has given rise to the field of cyber criminology, which investigates the motivations behind crimes committed in digital environments and their repercussions in the physical world.

To effectively counter cyber threats, it is essential for Indian law enforcement to be equipped with adequate resources and specialized knowledge. An adaptable legislative framework is crucial and must be periodically updated to address emerging challenges. Additionally, a robust national cybersecurity strategy is vital for ensuring a secure and resilient digital environment for citizens, businesses, and governmental operations. This cybersecurity framework delineates vision, objectives, guiding principles, & methodologies necessary to achieve cybersecurity goals.

Furthermore, developing comprehensive modules for cybercrime investigations, training cybercrime investigators in both investigation techniques and forensics, and ensuring the availability of essential equipment through state forensic science laboratories are critical components for effective cybercrime policing. Hence, the current landscape of cyber policing and investigation demands heightened professionalism, enhanced confidentiality, increased reliance on automated technologies, and a nuanced understanding of the complexities inherent in the digital realm.

*****

[94] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

ADDRESSING THREATS TO CYBERSECURITY UNDER DATA PROTECTION LAWS IN INDIA: AN ANALYSIS

Ashutosh Kumar Gautam[95]

ABSTRACT

In recent years, India's rapid digital transformation has heightened the risk of cyber threats, creating challenges for protecting personal data, ensuring privacy, and safeguarding national security. This abstract provides an in-depth analysis of the intersection between cybersecurity risks and India's data protection laws, particularly with the enactment of the Digital Personal Data Protection Act, 2023. The new law represents a significant step toward enhancing individual privacy rights and enforcing data protection standards, but it also raises concerns about how effectively it can address the growing cybersecurity threats in an interconnected digital environment. The analysis reviews the effectiveness of India's legal framework in mitigating cybersecurity risks, including data breaches, cyber espionage, ransomware, and other emerging cyber threats. It explores the regulatory mechanisms outlined in the data protection law, focusing on how companies and government bodies are required to implement cybersecurity protocols, report breaches, and comply with data protection mandates. The role of the Data Protection Board of India in overseeing enforcement and ensuring accountability for both private and public entities is also discussed. Despite the legal advancements, challenges persist in enforcing cybersecurity standards, addressing cross-border data transfers, and raising cybersecurity awareness. The paper highlights the need for greater cooperation between government authorities, tech companies, and international regulatory bodies to counteract the evolving threat landscape. In conclusion, while the Digital Personal Data Protection Act provides a robust foundation for data protection, it must be complemented by a comprehensive, multi-stakeholder approach to effectively address the complex cybersecurity challenges facing India in the digital age.

Keywords: Data Protection, Cyber Security, Data Privacy, Digital era, Law enforcement

INTRODUCTION

Seamless flow of information is a unique feature of this modern interconnected world where all the essential things are now available through online mediums, the importance of cyber security has become paramount.[96] The uncontrolled growth of technologies and delays in framing of cyber security laws have highly increased the threat of cyber crimes to happen. High dependency on cyber technologies and poor implementation of cyber security measures creates a good atmosphere for cyber attacks.[97]

Cyber security is essential for safeguarding sensitive information, maintaining business continuity, and protecting individuals and organisations from financial loss and reputational damage. Hackers & cybercriminals constantly devise innovative tactics to exploit vulnerabilities, making it imperative to stay vigilant and adapt to evolving challenges.

Common Cyber Threats: Here are the details of some prominent cyber crimes[4]-

[95] Research Scholar at Department of Law, University of Lucknow, India.

[96] Ashwini Sheth, Sachin Shankar Bhosale and Farish Kurupkar, "Research Paper on Cyber Security" Special Issue *Contemporary research in India* 246 (2021).

[97] A. Saravanan and S. Sathya Bama, "A Review on Cyber Security and the Fifth Generation Cyberattacks" 12(2) *Oriental Journal of Computer Science and Technology* 50 (2019).

- **Malware:** Systems are infiltrated by malicious softwares and which causes operations to become disrupted; it also results in stealing of data, or holding systems hostage for ransom. Apart from viruses, other notable examples of malware are worms, spyware, trojans and ransomware.
- **Phishing:** Deceptive tactics used to trick users to reveal their sensitive information. Phishing attacks often mimic legitimate organisations to gain trust and deceive victims.
- **Denial-of-Service (DoS):** For making the system non usable this attack is done by overwhelming a system or network with traffic. Attacks can disrupt critical services and damage an organisation's reputation.
- **Data Breaches:** Accessing personal or secret information in an unauthorised way which makes individuals and organisations to face problems & loss, including legal liabilities and loss of customer trust.

Best Practices for Cyber Security: Many people are not aware or fail to utilise the basic/needed cyber security measures and they easily become victims of cyber crimes.[98] Some basic cyber security measures are:

- **Strong Passwords**
- **Software Updates**
- **Firewall Protection**
- **Antivirus Software**
- **Backup Data**
- **Employee Training**
- **Incident Response Plan**

By implementing these measures and by regularly checking the cyber security trends & adopting proactive measures of security, individuals and organisations have to continuously care about their cyber security posture & minimise the risks of cyber threats.

CYBER RISKS AND THREATS: A GROWING CHALLENGE

The digital age has also brought forth a complex landscape of cyber threats.[99] These threats, often evolving at a rapid pace, pose significant risks to individuals, organisations, and critical infrastructure. Through unauthorised access or through cyber attacks a target system can be illegally controlled.[7] Common Cyber Threats and their Implications

[98] D. Phillips, "Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies" 2(2) Forensic Sciences 379-398.(2022).

[99] Dr. Khyati Tejpal, Dr. D.Y. Patil Vidyapeeth, Dr. Jayashree Patole, Dr. D.Y. Patil Vidyapeeth, Tanmay Ghugare, and Dr. D.Y. Patil Vidyapeeth, "CYBERSECURITY: PRESSING PRIORITY IN INDIA" 11(2) *The Online Journal of Distance Education and e-Learning* 2052 (2023)..

- **Malware:** As said above malware disrupts operations performed by a system. Ransomware attacks, in particular, have paralysed businesses and critical services, demanding hefty ransom payments for data decryption.
- **Phishing Attacks:** These deceptive tactics exploit human psychology, luring victims through emails, SMSes, social media posts. Successful phishing attacks results in identity theft, reputational damage and financial frauds.
- **Denial-of-Service (DoS):** DoS attacks make websites & online services inaccessible which disrupts business operations & forces victims to face financial losses.
- **Data Breaches:** This unauthorised act forces compromise privacy, financial information and also causes loss to the value of intellectual property.
- **Advanced Persistent Threats (APTs):** State-sponsored or highly organised cybercriminal groups employ sophisticated techniques to infiltrate networks, steal valuable data, and maintain long-term access. APTs often target critical infrastructure, government agencies, and businesses in strategic sectors.

Mitigating Cyber Risks: A Multi-Layered Approach: In the modern era the government as well as a single individual are continuously under the threat of cyber crimes.[100] To effectively combat cyber threats, a comprehensive and proactive approach is essential. Key strategies and measures of security gave been explained above. Training & awareness are some one of the most crucial steps including recognising attempts of phishing, avoiding links or attachments which are suspicious & practising safe browsing habits, is essential to building a strong security culture. Response planning regarding any cyber crime can help organisations respond effectively to cyberattacks, minimising damage and accelerating recovery efforts. Cybersecurity insurance is also very helpful. Investing in cybersecurity insurance can provide financial protection against losses resulting from cyber incidents. By adopting these strategies, individuals/organisations can bolster their cyber defenses and safeguard their digital assets.

CYBER SECURITY IN INDIA: A GROWING CHALLENGE

India, a nation rapidly embracing digital transformation, finds itself increasingly exposed to a complex and evolving cyber threat landscape. As the country integrates technology into every facet of life, from government services to personal finance, the stakes for cyber security have never been higher. It is also a point that the increasing number of cyber attacks and threat of cyber risk has been warning everyone and due to this alertness cyber security mechanism is improving[101] but still more efforts have to be made to strengthen the cyber security system.[102]**The Evolving Threat Landscape:** Cybercriminals are drawn to India's large population, burgeoning digital economy, and critical infrastructure. This makes the country a prime target for a variety of cyberattacks, including:

[100] Aadil Ahmad Shairgojri, Showkat Ahmad Dar, "Emerging Cyber Security India's Concern and Threats" 2(4) *International Journal of Information technology and Computer Engineering* 17 (2022).
[101] *Supra* note 81 at 55.
[102] K. Gupta, "Importance of cybersecurity in India" 5(3) *International Journal of Engineering Research* 27 (2018).

- **Data Breaches:** High-profile data breaches have exposed the personal and financial information of millions of Indian citizens, compromising trust in digital systems.
- **Phishing Attacks:** Sophisticated phishing scams, often disguised as legitimate communications from trusted institutions, continue to deceive unsuspecting individuals into divulging sensitive information.
- **Ransomware Attacks:** Ransomware attacks have crippled businesses and critical infrastructure, demanding substantial ransom payments to restore access to encrypted data.
- **Advanced Persistent Threats (APTs):** State-sponsored and highly organised cybercriminal groups employ advanced techniques to infiltrate networks, steal valuable data, and disrupt operations.

Government Initiatives & challenges: The Indian government has recognised the gravity of cyber threats and has taken several steps to bolster the country's cyber defences:

- **National Cyber Security Strategy:** This comprehensive strategy provides a roadmap for creating a secure and resilient cyberspace, addressing various aspects of cyber security, from policy and regulation to technology and capacity building.
- **Indian Computer Emergency Response Team (CERT-In):** CERT-In serves as the nodal agency for responding to cyber security threats and incidents, coordinating with various stakeholders to mitigate risks and minimise damage.
- **Cyber Security Capacity Building:** The government has invested in initiatives to enhance the cyber security skills of IT professionals and law enforcement agencies, equipping them with the knowledge and tools to combat cyber threats effectively.
- **Public Awareness Campaigns:** These are organised to inform citizens about managing cyber risks, preventing cyber threats & understanding the role of cyber hygiene.

For dealing with the issue of cyber crimes various measures have been taken in India.[103]However, India still faces significant challenges in its pursuit of a secure digital future:

- **Skill Gap:** A shortage of skilled cyber security professionals hinders the country's ability to respond effectively to complex cyberattacks and implement robust security measures.
- **Outdated Infrastructure:** Many organisations, particularly in critical sectors like healthcare and finance, still rely on outdated technology that is vulnerable to exploitation.
- **Lack of Awareness:** A significant portion of the population remains unaware of the nature of cyber threats. Lack of knowledge of how to protect themselves, makes vulnerable people easy targets.
- **Complex & evolving regulatory landscape:** This can sometimes hinder effective cyber security implementation, creating confusion and delays in adopting necessary security measures.

[103] S. Supriya, "CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS" 7(6) International Journal of Mechanical Engineering (2022).

To address these challenges and build a more secure digital India, several key steps are essential:

- **Invest in Cyber Security Infrastructure:** Allocate significant resources to upgrade IT infrastructure, deploy advanced security solutions, and implement robust security protocols.
- **Promote Cyber Security Education and Training:** Foster a strong cyber security workforce by investing in education and training programs at various levels, from primary schools to higher education institutions.
- **Strengthen International Cooperation:** Collaborate with other countries to share information, best practices, and intelligence on emerging cyber threats, fostering global cooperation in the fight against cybercrime.
- **Raise Public Awareness:** Continuous education of cyber hygiene through awareness campaigns, workshops, and educational materials.
- **Foster a Culture of Cyber Hygiene:** Encourage individuals and organisations to adopt strong practices of cyber hygiene.

By taking these measures, India can strengthen its cyber defences, protect its critical infrastructure, and safeguard the digital future of its citizens.

A GLOBAL EFFORT TO COMBAT CYBERCRIME

The rise of cybercrime has necessitated international collaboration to address this complex and evolving threat. A multitude of international organisations, governments, and private sector entities have joined forces to develop strategies, share information, and implement measures to combat cyber threats. Key International Initiatives are as follows:[104][105]

The Council of Europe Convention on Cybercrime (Budapest Convention) provides a legal framework for international cooperation in investigating and prosecuting cybercrime. It covers a wide range of cybercrimes, including hacking, computer fraud, child pornography, and cyberterrorism. The Convention encourages countries to adopt legislation criminalising cybercrime and to cooperate in investigations and prosecutions.

While significant progress has been made in international cooperation against cybercrime, the challenge remains complex and ever-evolving.[106] Continued collaboration, innovation, and adaptation are essential to stay ahead of cyber threats and protect the global digital landscape.

The **G7 and G20** groups of major economies have recognised the importance of cybersecurity and have issued joint statements and declarations on the issue. They have emphasised the need for international cooperation, information sharing, and capacity building to combat cyber threats.

[104] S. Mali, "ANALYSING THE AWARENESS OF CYBER CRIME AND DESIGNING A RELEVANT FRAMEWORK WITH RESPECT TO CYBER WARFARE: AN EMPIRICAL STUDY"
[105] (2) International Journal of Mechanical Engineering and Technology 110-124 (2018).
[106] S. Devi, "Cyber Security In The National Security Discourse" 23(2) *World Affairs: The Journal of International Issues* 146-159. (2019)

Interpol: Coordinating efforts of international law enforcement to deal with cybercrimes. Information sharing is facilitated, it provides technical assistance, and conducts joint operations to apprehend cybercriminals.

The **United Nations** has recognised the global nature of cybercrime and has adopted resolutions calling for international cooperation to address the issue. The UN Office on Drugs and Crime (UNODC) works to strengthen the capacity of member states to investigate and prosecute cybercrime.

International Cooperation: Sharing information and intelligence between countries is essential to track cybercriminals and disrupt their activities. Joint investigations and operations can help dismantle cybercrime networks and bring perpetrators to justice.

Legal Cooperation: Harmonising national laws and developing international legal frameworks can facilitate cross-border investigations and extraditions. International cooperation agreements can streamline the process of requesting and providing evidence.

Capacity Building: The stakeholders who provide justice have to be trained. Police system & judiciary have to become advanced which can help countries improve their cybersecurity capabilities.

Public-Private Partnerships: Collaboration between governments, industry, and academia is essential to develop effective cybersecurity strategies. Sharing information and best practices can help identify and mitigate emerging threats.

Cybersecurity Standards and Best Practices: Developing and promoting international standards for cybersecurity can help ensure consistency and interoperability. Encouraging the adoption of best practices can improve the overall level of cybersecurity.

INDIA'S FIGHT AGAINST CYBERCRIME: A COMPREHENSIVE APPROACH

"Computers, networks, data, and other digital assets are protected from unauthorised access, theft, damage, and other hostile actions by means of practises, processes, and technology known as cybersecurity."[107] India, like many other nations, has been increasingly grappling with cyber threats. To address this growing challenge, the Indian government has implemented various measures to strengthen cybersecurity and combat cybercrime. Key Indian Government Initiatives:[15]

Indian Computer Emergency Response Team (CERT-In): This nodal agency has a crucial role to play in responding to cyber security threats & incidents. CERT-In monitors cyber threats, issues alerts and advisories, and coordinates with various stakeholders to mitigate risks and minimise damage. It conducts vulnerability assessments, security audits & capacity building programs.

National Cyber Security Strategy: This comprehensive National Cyber Security Strategy has been made by the government to create a secure and resilient cyberspace. This strategy outlines a roadmap for addressing various aspects of cybersecurity, including policy and regulation, technology, and capacity building. It emphasises cooperation at international level, public-private partnerships & research and development in cybersecurity.

[107] *Supra* note 85 at 2055.

Cyber Security Capacity Building: The government has invested in initiatives to enhance the cybersecurity skills of IT professionals and law enforcement agencies. This includes training programs, workshops, and certifications to equip individuals with the knowledge and tools to combat cyber threats effectively. The government has also established specialised cybersecurity training centres and academic programs to nurture a skilled cybersecurity workforce.

Public Awareness Campaigns: These campaigns aim to empower individuals to protect themselves from cyberattacks. The government has also developed user-friendly guidelines and tools to help individuals and organisations adopt strong cybersecurity practices.

Information Technology Act, 2000: This Indian cyber security legal framework has been amended several times to address emerging cyber threats and to enhance penalties for cybercrimes. The Act covers a wide range of cybercrimes, including hacking, data theft, cyber terrorism, and online fraud.

Personal Data Protection Act, 2018: Processing of personal data is regulated under this newly passed Act and the aim is to secure the privacy of people by imposing obligations to protect personal data.

Challenges & Future Directions: Despite these efforts, India continues to face significant challenges. These challenges include a shortage of skilled cybersecurity professionals, outdated infrastructure, and a lack of awareness among the public.[108] To address these challenges, India needs to:[109]

- **Invest in Cybersecurity Infrastructure:** Allocate significant resources to upgrade IT infrastructure, deploy advanced security solutions, and implement robust security protocols.
- **Promote Cybersecurity Education and Training:** Foster a strong cybersecurity workforce by investing in education and training programs at various levels, from primary schools to higher education institutions.
- **Strengthen International Cooperation:** Collaborate with other countries to share information, best practices, and intelligence on emerging cyber threats, fostering global cooperation in the fight against cybercrime.
- **Raise Public Awareness:** Continuously educate people about cyber hygiene through awareness campaigns, workshops, and educational materials.
- **Foster a Culture of Cyber Hygiene:** Encourage individuals and organisations to adopt strong cyber hygiene practices and regularly backing up important data.

By taking these measures, India can strengthen its cyber defences, protect its critical infrastructure, and safeguard the digital future of its citizens.

INDIA'S DATA PROTECTION LANDSCAPE: A DEEP DIVE INTO THE DIGITAL PERSONAL DATA PROTECTION ACT

[108] *Supra* note 88 at 22.
[109] N.A.H.A Alık,(2022), "Emerging Cyber Security Threats: India's Concerns and Options" 4(1) *International Journal of Politics and Security* 170-200 (2022).

India's Digital Personal Data Protection Act (DPDPA)[110] marks a significant stride in safeguarding individual privacy in the digital age. This new law aims to balance the interests of individuals, businesses, and the government in the ever-evolving digital landscape.

Individual Rights Under the DPDPA: The DPDPA empowers individuals with several rights, including:

- **Right to Information:** to obtain information alto know about processing of their personal data.
- **Right of Access:** access their personal data held by organisations.
- **Right to Correction:** request for the correction of incomplete/wrong personal data.
- **Right to Erasure:** request the erasure if an individual deems fit as per law.
- **Right to Object:** object to the processing in specific cases of their personal data.
- **Right to Data Portability:** right to receive their personal data in a structured, commonly used & machine-readable format and transmit it to another controller.

Implications for Businesses: The DPDPA imposes significant obligations on businesses operating in India. organisations must comply with the Act's provisions, including conduction assessments of the impacts of data protection, implementation of robust policies of data protection & appointment of data protection officers. Failure in compliance leads to hefty fines, penalties and reputational damage. Key compliance considerations for businesses are as follows:

- **Data Mapping:** Conduction of a comprehensive inventory of personal data collected, processed & stored.
- **Consent Mechanism:** Implement clear and transparent consent mechanisms.
- **Data Security:** Implementation of security measures like encryption, control of access & audits of security measures regularly.
- **Data Breach Notification:** A robust incident response plan which can notify individuals amd relevant authorities if a case of a data breach arises.
- **Cross-Border Data Transfers:** Ensure compliance with cross-border data transfer regulations and implement appropriate safeguards.

The DPDPA represents a significant step forward in India's data protection landscape. By understanding and adhering to its provisions, businesses can not only protect themselves from legal risks but also build trust with their customers. As the digital landscape continues to evolve, staying updated on the latest developments in data protection law and adopting proactive measures is essential for organisations operating in India.[111]

CONCLUSION AND SUGGESTIONS

In conclusion, it is appropriate to say that India desperately needs strong cybersecurity measures. To effectively combat cyber threats, a multifaceted approach is imperative, involving international

[110] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
[111] *Supra* note 86 at 2060.

cooperation, strong laws, programmes for capacity building, technological advancements, public awareness and effective incident response.

Key recommendations to strengthen cybersecurity:

1. **International Cooperation:**

- Foster international collaboration to share information, best practices, and intelligence on emerging cyber threats.
- Establish joint investigative teams to dismantle cybercrime networks and bring perpetrators to justice.
- Harmonise national laws and develop international legal frameworks to facilitate cross-border investigations and extraditions.

2. **Strong Legal Framework:**

- Enact comprehensive cybersecurity legislation to address the evolving nature of cybercrime.
- Impose stringent penalties on cybercriminals to deter malicious activities.
- Establish robust data protection laws to safeguard personal information.

3. **Capacity Building:**

- Invest in cybersecurity education and training programs to develop a skilled workforce.
- Promote cybersecurity awareness amongpeople including children & the elderly.
- Collaborate with academic institutions to conduct research and develop innovative cybersecurity solutions.

4. **Public Awareness:**

- Encourage using strong passwords, enable multi-factor authentication & be cautious of phishing attacks.
- Promoting regular software updates & security patches.

5. **Robust Cybersecurity Infrastructure:**

- Implement strong access controls, like firewalls & intrusion detection systems.
- Conduction of regular security audits & assessments of vulnerability.
- Utilise artificial intelligence to detect cyber risk & vulnerabilities.

6. **Data Protection:**

- data minimization, encryption & regular backups are some strong measures.
- Comply with data protection regulations.

7. **Incident Response Planning:**

- Establishment of incident response teams to handle cyber incidents promptly and efficiently.
- Conduct regular cybersecurity drills to test incident response procedures.

8. **Public-Private Partnerships:**

- Foster collaboration between governments, industry, and academia to share information, best practices, and resources.
- Encourage the development of cybersecurity standards and certifications.
- Support the creation of cybersecurity innovation hubs and incubators.

In recent years, India's rapid digital transformation has heightened the risk of cyber threats, creating challenges for protecting personal data, ensuring privacy, and safeguarding national security. This paper provides an in-depth analysis of the intersection between cybersecurity risks and India's data protection laws, particularly with the enactment of the Digital Personal Data Protection Act, 2023. The new law represents a significant step toward enhancing individual privacy rights and enforcing data protection standards, but it also raises concerns about how effectively it can address the growing cybersecurity threats in an interconnected digital environment.

*****

ADDRESSING JURISDICTIONAL CHALLENGES IN COMBATTING CYBER CRIMES: PATHWAYS FOR THE FUTURE

Dr. Atul Jaybhaye[112]

ABSTRACT

With the rapid advancement of digitization and technology, the usage of e-commerce, social media platforms, online banking, and digital communication services has surged among Internet users. Consequently, the last few years have witnessed a significant rise in cybercrime. In 2022, India recorded a 24% increase in cybercrime cases compared to 2021, according to the "National Crime Records Bureau (NCRB)." This rise occurred alongside increases in other types of crime, such as economic offences (11%), crimes against senior citizens (9%), and crimes against women (4%). While "the Information Technology Act, 2000" (IT Act, 2000) does not specifically define the term 'cybercrime,' it is generally understood as any crime in which a computer serves as either a tool or a target. Cybercriminals are constantly evolving their tactics, employing increasingly sophisticated methods to perpetrate fraud and other illegal activities. Although law enforcement agencies are working diligently to investigate these crimes, they face numerous challenges—foremost among them is determining jurisdiction in cybercrime cases. Jurisdictional criteria vary widely between countries, and the IT Act, 2000, provides limited guidance on the matter, addressing jurisdiction primarily through Section 75. Moreover, recent legislative measures such as the "Bharatiya Nyaya Sanhita, 2023," (BNS) and the "Bharatiya Nagarik Suraksha Sanhita, 2023", (BNSS) offer little in the way of resolving jurisdictional issues in cyberspace. Consequently, the Indian judiciary often relies on legal tests and theories developed in U.S. jurisprudence, such as the "Minimum Contacts Theory," "Sliding Scale Theory," and the "Effects Test", to determine jurisdiction in cybercrime cases. This paper critically analyzes the jurisdictional challenges faced in the investigation of cybercrimes and offers recommendations to effectively address these issues, thereby enhancing the ability of law enforcement and judicial systems to combat cybercrime in the future.

Keywords: Cybercrime, Jurisdiction, IT Act, 2000, Digital investigation, Minimum Contacts Theory

INTRODUCTION

The age of information technology has profoundly transformed human life. The internet has become an essential part of daily existence, spanning all age groups from children to the elderly. Notably, even the Hon'ble Supreme Court of India has acknowledged the significance of internet access, affirming it as a fundamental right that cannot be unjustly denied.[113] With the rapid progress of digitization, the use of e-commerce, social media platforms, online banking, and digital communication services has surged among Internet users. However, technology acts as a double-edged sword, bringing both benefits and drawbacks. While many individuals harness technology for lawful and productive purposes, cybercriminals exploit it to commit various offenses, including phishing, child pornography, cyber terrorism, and the creation of deepfake videos. Consequently, the past few years have seen a significant rise in cybercrime. In 2022, India recorded a 24% increase in cybercrime cases compared to 2021, as per the (NCRB). This spike coincided with increases in other crimes, such as economic offenses (11%),

[112] Assistant Professor (Law), Hidayatullah National Law University, Raipur, Chhattisgarh.

[113] Available at "https://www.indiatoday.in/news-analysis/story/internet-access-fundamental-right-supreme-court-makes-official-article-19-explained-1635662-2020-01-10" (last visited on September 9, 2024).

crimes against senior citizens (9%), and crimes against women (4%).[114] Despite the diligent efforts of law enforcement agencies to combat cybercrime, they face considerable challenges, particularly in determining jurisdiction. Jurisdictional criteria vary between countries, and when a cybercrime is committed by a foreign national targeting a computer system in India, jurisdictional complexities often arise. Law enforcement agencies and courts frequently struggle to ascertain the appropriate jurisdiction and the applicable laws, rules, and regulations, as these crimes occur in the virtual realm of cyberspace.

CONCEPT OF JURISDICTION

Jurisdiction is derived from two Latin terms: "*juris* (meaning law) and *diction* (meaning to speak)." Essentially, jurisdiction answers the question of which forum is appropriate and has the authority to "speak the law." According to "Black's Law Dictionary", jurisdiction refers to "a court's power to resolve a case or issue a decree." The concept of jurisdiction exists to ensure that courts only handle matters that are within their legitimate scope, whether based on territorial boundaries or financial thresholds. Jurisdiction is rooted in public international law, conflict of laws, constitutional law, and the powers of the government's executive and legislative branches to allocate resources in a way that best serves societal needs.[115]

JURISDICTION IN CYBERSPACE

In cyberspace, jurisdiction poses a significant challenge for both domestic and international courts. If cyberspace is not treated as a global domain, it complicates traditional conflict-of-law principles, rendering them ineffective. Unlike conventional jurisdictional disputes, which may involve a few conflicting legal systems, even a basic webpage can be subject to the laws of multiple jurisdictions. To address this, cyberspace jurisdiction demands well-defined principles based on international law. Only by adopting such principles can courts worldwide work toward uniform solutions for resolving Internet jurisdiction issues.[116]

"The scope of cyber law is so extensive that defining jurisdiction in cases involving multiple countries can be very challenging. What may be legal in one country—whether it is a website, app, product, or content—could be illegal in another. Additionally, the parties involved could be residents or non-residents, further complicating the issue. Cyber jurisdiction is typically determined by the nature of the cybercrime and the location from which it was committed. Jurisdiction grants authority to the relevant court to hear a case and deliver a verdict. In cybercrime cases, the victim and the accused are often located in different countries, leading to conflicts over which jurisdiction should apply. While users are generally free to access content from anywhere, jurisdiction becomes critical when their online activities cross into illegal or criminal territory."[117]

---

[114] Available at "https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/" (last visited on September 9, 2024).
[115] Mr. Amit Karkhanis, "An Overview of The Concept of Jurisdiction", available at https://www.livelaw.in/law-firms/articles/concept-of-jurisdiction-173713 (last visited on September 11, 2024).
[116] Darrel C. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces," 4 *Michigan Telecommunications and Technology Law Review*, 70 (1998).
[117] Available at "https://lawbhoomi.com/jurisdictional-aspects-in-cyber-law-and-information-technology-act/" (last visited on September 13, 2024).

Traditionally, jurisdiction is determined by where the cause of action arises, but in cases involving multiple parties from different parts of the world, this becomes complicated. In cyberspace transactions, there are typically three key parties: the user, the service provider, and the person or business involved in the transaction. Ideally, the most appropriate legal framework should determine whether an event in cyberspace is governed by the laws of the state or country where the user is located, or if the laws of all other relevant countries or states should also apply. Unlike conventional transactions, cyber interactions involve the user, the server host, and the party with whom the transaction occurs, raising the fundamental question: which country's law should prevail?

Key issues arise when determining:

- In cross-border interactions, on what basis do we determine which country's law applies and which court has jurisdiction?
- What criteria allow a nation to apply its laws and regulations when the internet activity originates from a different jurisdiction?

In such cases, matters of jurisdiction fall under both state and international law, particularly when the parties involved are from different nations. Under international law, a state can apply its legal framework when international parties are involved in a dispute.[118]

TYPES OF JURISDICTIONS

International law identifies three types of jurisdictions in cyberspace:

Personal Jurisdiction – This type of jurisdiction permits a court to issue judgments specifically over certain individuals or parties. In ***Pennoyer v. Neff***, the U.S. Supreme Court ruled that the Due Process Clause of the U.S. Constitution limits the exercise of personal jurisdiction over non-residents, meaning courts generally cannot assert direct jurisdiction over individuals who do not reside within the state. However, this limitation was later modified by the "minimum contacts" theory, which permits courts to exercise jurisdiction over non-residents if they have enough connections or interactions with the state.

Subject-matter jurisdiction – This type of jurisdiction allows a court to decide cases related to specific subject matters. If a case is filed in a court that does not have jurisdiction over the particular subject matter, the case will be dismissed, and the plaintiff must be refiled in the appropriate court. For example, a complaint concerning a consumer product must be filed in a district consumer forum, which specializes in consumer-related cases, rather than in a district court. Similarly, environmental disputes are handled by the National Green Tribunal (NGT), not by district courts, as the NGT has exclusive jurisdiction over environmental matters.

Pecuniary Jurisdiction – This type of jurisdiction pertains to financial matters, specifically where the value of a suit must fall within the court's pecuniary limits. Courts have defined monetary thresholds, and cases exceeding these limits must be tried in higher courts. For example, the district consumer forum handles disputes involving amounts up to ₹20 lakh, the State Consumer Dispute Redressal

[118] Ms. Prevy Parekh & Ms. Tarunya Rao, "Cyberspace and Jurisdiction", 2 *Journal on Contemporary Issues of Law* 5 (2016).

Commission handles cases exceeding ₹20 lakh but below ₹1 crore, and the National Consumer Dispute Redressal Commission addresses cases involving amounts over ₹1 crore in India. This system is structured hierarchically based on the claim's value in the proceedings.[119]

Legal framework of Jurisdiction in India:

Extraterritorial jurisdiction – Cybercrimes: (Bharatiya Nyaya Sanhita, 2023)

"The provision of this Sanhita also apply to any offence committed by—

(a) any citizen of India in any place without and beyond India;

(b) any person on any ship or aircraft registered in India wherever it may be; and

(c) any person in any place without and beyond India committing offence targeting a computer resource located in India.[120]

Explanation - In this section, the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Sanhita."

"The Information Technology Act, 2000"

"Sec. 75 – Act to apply for offence or contravention committed outside India." -

(1) "Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."[121]

Sec. 75 of the IT Act, 2000 has a broader scope compared to Sec. 1(5) of the BNS, 2023. Section 75 applies to offences committed abroad involving a computer, computer system, or computer network located in India, while the BNS limits jurisdiction to cases where the targeted computer resource is within India. However, Sec. 75 has its limitations. For instance, if an offence under the IT Act is committed by a foreign national outside India and affects a computer system in India, but the act is not considered an offence in that foreign country, an Indian court's judgment may not be enforceable in that foreign jurisdiction. This is because the foreign court may not recognize the extraterritorial jurisdiction outlined in Sec. 75 if the act is legal in that country.[122]

Sec. "199 -Offence triable where act is done or consequence ensues." ("Bharatiya Nagarik Suraksha Sanhita, 2023")

"When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a Court within whose local jurisdiction such thing

[119] *Supra* note 5.
[120] Bharatiya Nyaya Sanhita, 2023, s. 1(5).
[121] The Information Technology Act, 2000, s. 75.
[122] Nishant Verma, Jurisdiction in Cybercrimes and Civil Disputes, available at "https://www.scconline.com/blog/post/2024/03/24/jurisdiction-in-cybercrimes-and-civil-disputes/"(last visited on September 17, 2024).

has been done or such consequence has ensued."

Sec. 202 – "Offences committed by means of electronic communications, letters," etc. (BNSS 2023)

"(1) Any offence which includes cheating, may, if the deception is practised by means of electronic communications or letters or telecommunication messages, be inquired into or tried by any Court within whose local jurisdiction such electronic communications or letters or messages were sent or were received; and any offence of cheating and dishonestly inducing delivery of property may be inquired into or tried by a Court within whose local jurisdiction the property was delivered by the person deceived or was received by the accused person.

(2) Any offence punishable under section 82 of the Bharatiya Nyaya Sanhita, 2023 may be inquired into or tried by a Court within whose local jurisdiction the offence was committed or the offender last resided with his or her spouse by the first marriage, or the wife by the first marriage has taken up permanent residence after the commission of the offence."

THE EVOLUTION OF JURISDICTIONAL TESTS IN U.S. JUDICIAL PRACTICE

1. Minimum Contacts Theory

This test is applicable when either or both parties are located outside the court's territorial jurisdiction. In the landmark judgment in "***Washington v International Shoe Company"***,[123] this theory was originated by the US Supreme Court.[124]

After this case, the court has come up with three criteria-

- "The non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections.
- the claim must be one that arises out of or results from the defendant's forum-related activities, and
- exercise of jurisdiction must be reasonable."

In the case of "***CompuServe Inc v Patterson"***[125], The court ruled that contracts involving cyberspace are also subject to the minimum contacts theory.

2. Sliding Scale Theory

"The Sliding Scale theory, commonly referred to as the Zippo Test, is a widely accepted framework for determining personal jurisdiction in cyberspace cases. This test assesses the level of interactivity of websites to establish jurisdiction. Generally, the more interactive a website is, the greater the likelihood that courts will assert personal jurisdiction over it in the forum state. For passive websites, courts

[123] 326 US 310 (1945).
[124] Karnika Seth, "Jurisdiction in the Borderless Cyberspace", available at "http://www.karnikaseth.com/wp-content/uploads/Karnika%20Seth's%20Computers%20Inernet%20%20New%20Technology%20Laws.pdf"(last visited on September 17, 2024).
[125] 89F 3d 1257(6th Cir1996).

typically have little to no jurisdiction. In cases of websites that fall somewhere in the middle, jurisdiction may be uncertain, while highly interactive sites usually grant courts clear jurisdiction in cyberspace."[126]

In the landmark case of "***Zippo Manufacturer v Zippo.Com"***[127], the plaintiff Zippo Manufacturer of lighters in Pennsylvania filed a suit against the defendant Zippo.com for trademark violation. The defendant had sufficient interactivity; therefore, the personal jurisdiction was made applicable to the defendant.

3. Effects Test and International Targeting

To satisfy the Effect test, certain conditions must be fulfilled: primarily, the action should be directed precisely at the forum state with the knowledge and intent to cause harm there. If the court decides that the defendant's actions have indeed caused injury to the forum state, it can assert personal jurisdiction in cyberspace cases even when there are no direct contacts. This approach allows courts to extend their jurisdiction based on the foreseeable effects of a defendant's conduct on the forum state, emphasizing the impact of the action rather than the location of the parties involved.

In the famous case of "***Calder v Jones"***[128], the U.S. Supreme Court held that a court can exercise personal jurisdiction over non-residents in certain cases. In the case of *Shirley Jones*, she filed the suit against the distributor, writer, and editor of a national magazine for defamation after they labeled her an alcoholic. Albeit, the article was written and edited in Florida, Jones filed her lawsuit in California due to the magazine's substantial distribution there. The court ruled that California had personal jurisdiction over the defendants, highlighting the article's impact within the state.

In *"**Panavision International v Toeppen"**,*[129]

The defendant was engaged in cybercrime by using the plaintiff's trademark commercially and attempting to sell it back to him at a high price. The California court applied the effects test and ruled that it had personal jurisdiction over the non-resident defendant due to the intentional harm caused to the plaintiff in California.

OTHER COMMON LAW JURISDICTIONS

Next, we will examine the approach taken by courts in other common law jurisdictions, including India.[130]

Canada

In "***Morguard Investments Ltd. v. De Savoye***,"[131] the Canadian Supreme Court established the "real and substantial connection" test for ascertaining jurisdiction. The court noted that allowing a suit to proceed based on this connection strikes a fair and reasonable balance between the rights of the parties involved. In "***Pro-C Ltd. v. Computer City Inc."***[132] the court ruled that the defendant's listing of

[126] *Supra* note 5.
[127] 952 F Supp 1119 (DCWD Pa 1997).
[128] 465 US 783 (1984).
[129] 141 F 3d 1316 (9th Cir1998).
[130] Justice S. Muralidhar, "Jurisdictional Issues in Cyberspace," *Indian Journal of Law and Technology*, 6, 22-26, (2010).
[131] [1990] 3 S.C.R. 1077 (Can.).
[132] 7 C.P.R. (4th) 193 (Can.), rev'd, 205 D.L.R. (4th) 568 (Can.).

Canadian retail outlets on their website, combined with the existence of a de facto "common market" between Canada and the U.S., indicated that Canadian consumers were targeted. As a result, the Ontario court had jurisdiction to hear the trademark voilation case against the defendant based in the U.S.

In "***Patrick Desjean v. Intermix Media Inc.*"**[133] "The defendant, a Delaware corporation with its principal office in Los Angeles, offered seemingly free software programs. When the plaintiff, a Canadian resident, installed a free screensaver or game from www.mycoolscreen.com, he unintentionally also installed spyware. Subsequently, the plaintiff filed a lawsuit against the defendant in Canada for violating the misleading representations provisions of the Canadian Competition Act, 1985." The Federal Court of Ottawa, after stating to the decision of the Ontario Court of Appeal in "***Muscutt v. Courcelles,"*** (2002) 213 D.L.R. (4th) 577, considered the following eight factors to determine whether it had jurisdiction:

(1) "The connection between the forum and the plaintiff's claim; (2) The connection between the forum and the defendant; (3) Unfairness to the defendant in assuming jurisdiction; (4) Unfairness to the plaintiff in not assuming jurisdiction; (5) Involvement of other parties to the suit; (6) The Court's willingness to recognize and enforce an extra-provincial judgment rendered on the same jurisdictional basis; (7) Whether the case is interprovincial or international in nature; (8) Comity and standards of jurisdiction, recognition and enforcement prevailing elsewhere."

The court noted that the defendant had no office in Canada, although it previously subsidized office space for contractors on two websites acquired by Intermix. Additionally, there were no servers in Canada for www.mycoolscreen.com; it was hosted on a server in California. The data revealed that 66% of downloads came from American users, while Canada accounted for only 2.5% to 5.3% of downloads. Given these factors, the Federal Court ruled that Canadian courts lacked jurisdiction over the defendant due to the absence of a substantial connection with the forum. Notably, the court recognized the importance of reciprocity in enforcing extra-provincial judgments, emphasizing that without it, exercising personal jurisdiction over extraterritorial defendants could be ineffective.[134]

United Kingdom

In "***1-800 Flowers Inc. v. Phonenames*** "[135]

The defendant was a UK-based phonebook company, while the plaintiff operated a flower delivery business accessible globally through its website. However, there was no evidence that UK residents had actually placed orders on the site. The argument was made that since the website was accessible from the UK, the defendant's use of the mark "1-800" constituted use in the UK. In the first appeal, the bench ruled that the mere accessibility of websites worldwide did not equate to trademark use in all those jurisdictions. The court emphasized that the website owner's intention and how users would interpret

[133] 2006 F.C. 1395 (Can.).
[134] *Supra* note 18.
[135] [2002] F.S.R. 12 (C.A.) (U.K.).

the website were relevant factors. The Court of Appeals also dismissed the argument, with Justice Buxton noting that...

"I would wish to approach these arguments, and particularly the last of them, with caution. There is something inherently unrealistic in saying that A 'uses' his mark in the United Kingdom when all that he does is to place the mark on the internet, from a location outside the United Kingdom, and simply wait in the hope that someone from the United Kingdom will download it and thereby create use on the part of A. By contrast, I can see that it might be more easily arguable that if A places on the internet a mark that is confusingly similar to a mark protected in another jurisdiction, he may do so at his peril that someone from that other jurisdiction may download it; though that approach conjured up in argument before us the potentially disturbing prospect that a shop in Arizona or Brazil that happens to bear the same name as a trademarked store in England or Australia will have to act with caution in answering telephone calls from those latter jurisdictions. However that may be, the very idea of 'use' within a certain area would seem to require some active step in that area on the part of the user that goes beyond providing facilities that enable others to bring the mark into the area. Of course, if persons in the United Kingdom seek the mark on the internet in response to direct encouragement or advertisement by the owner of the mark, the position may be different; but in such a case the advertisement or encouragement in itself is likely to suffice to establish the necessary use."[136]

India:

"Casio India Co. Limited v. Ashita Tele Systems Pvt. Ltd".[137] "in this passing off action, the defendant operated a business in Bombay and had registered the domain name www.casioindia.com, with the second defendant serving as the Registrar for this domain. The plaintiff claimed to be a 100% subsidiary of Casio Computer Ltd. in Japan (Casio Japan), which owned the registered trademark "Casio" in India, and associated with various electronic products. The plaintiff had also registered multiple domain names in India, including "CasioIndiaCompany.com," "CasioIndia.org," and "CasioIndia.net." The first defendant obtained the contested domain name during a period when it held a distributorship agreement with the plaintiff." It was observed by the learned single Judge after referring to the decisions in ***Rediff Communication Ltd. v. Cyber Booth"***[138] and "***Dow Jones & Co. Inc. v. Gutnick"***[139] that "once access to the impugned domain name website could be had from anywhere else, the jurisdiction in such matters cannot be confined to the territorial limits of the residence of the defendant."[140] According to the learned single Judge, since a mere likelihood of deception, whereby an average person is likely to be deceived or confused was sufficient to entertain an action for passing off, it was not at all required to be proved that "any actual deception took place at Delhi. Accordingly, the fact that the website of Defendant No. 1 can be accessed from Delhi is sufficient to invoke the territorial jurisdiction of this Court."[141]

---

[136] *Ibid.*
[137] 2003 (27) P.T.C. 265 (Del.) (India), overruled by *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*, CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009) (India).
[138] A.I.R. 2000 Bom. 27 (India).
[139] (2002) H.C.A. 56 (Austl.).
[140] *Supra* note 25.
[141] *Ibid.*

In "***India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors****.",*[142] a different approach was adopted. India TV sued India Broadcast Live LLC for cybersquatting, alleging the defendants registered the domain name "indiatvlive.com," which was deceptively similar to the plaintiff's well-known trademark "India TV." The court held that domain names are subject to trademark law principles and ruled in favor of India TV, recognizing that the unauthorized use of the domain name amounted to passing off and infringement of intellectual property rights. The court granted a permanent injunction. It was also held that the mere fact that a website is available in a specific location might not be enough for the courts of that location to exercise personal jurisdiction over the website's owners. The situation would be different if the website was not only passive but also interactive, allowing browsers to not only access the contents but also subscribe to the services provided by the owners.

Both Casio and India TV were decisions of single Judges and required proper reconciliation. The opportunity presented itself in "***Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy"***[143] the plaintiff was a company located in Singapore. It claimed that it was part of a group of companies involved in the hospitality business. It claimed the use of the word mark 'Banyan Tree' and the banyan tree device since 1994. The plaintiff maintained the websites 'www.banyantree.com' and 'www.banyantreespa.com' since 1996. The websites were accessible in India. Its application for the registration of the mark and the device was also pending. In October 2007, the plaintiff learnt that the defendants, located in Hyderabad in Andhra Pradesh, had initiated work on a project under the name 'Banyan Tree Retreat', which according to the plaintiff was deceptively similar to that of the plaintiff. The plaintiff invoked the jurisdiction of the Delhi High Court, arguing that the defendants' website, www.makprojects.com/banyantree, which advertised their products and services, was accessible in Delhi. The plaintiff claimed that the use of a deceptively identical mark would mislead the public, thereby seeking an injunction. The Division Bench of the Delhi High Court, while addressing a referral from a Single Judge, affirmed its ruling in India TV and overruled Casio. The key issue was whether the Delhi court had jurisdiction, given that the defendant was based outside Delhi. The court established the "purposeful availment" test for online jurisdiction, stating that courts could assert jurisdiction if the defendant intentionally targeted customers in the plaintiff's jurisdiction, leading to harm there. Ultimately, the court dismissed the suit due to a lack of sufficient evidence showing targeting.

CONCLUSION

Addressing jurisdictional challenges in combatting cybercrimes under the IT Act, 2000 requires an understanding of how cyberspace defies traditional territorial boundaries. The Act provides a framework, but challenges remain due to the global nature of the internet. Jurisdiction is typically determined through three tests: the Territorial Nexus Test, where jurisdiction is based on a connection to the territory; the Effects Test, which grants jurisdiction if the crime significantly impacts a specific country; and the Targeting Test, where jurisdiction is determined if a cyber activity intentionally targets a particular region. However, these tests face limitations in a digital world, where hackers often operate across multiple jurisdictions, masking their locations and impacts. To overcome these obstacles, several

[142] 2007 (35) P.T.C. 177 (Del.) (India).
[143] CS(OS) 894/2008.

steps must be taken. First, the IT Act should be regularly updated to reflect new technological realities, including clearer guidelines for cross-border cybercrimes. International cooperation is essential, particularly through stronger agreements like Mutual Legal Assistance Treaties (MLATs) and adopting global frameworks such as the Budapest Convention. Furthermore, law enforcement must be equipped with advanced training and resources to tackle complex cybercrime investigations, particularly those involving cross-border issues. Collaboration with private tech companies is critical, as they hold vital data that can assist in tracking cybercriminals. Establishing effective public-private partnerships will help bridge the gap between law enforcement and the tech sector, expediting the investigative process. By focusing on updating legal frameworks, fostering international cooperation, and enhancing cybersecurity capabilities, the jurisdictional challenges in cybercrime investigations can be mitigated, ensuring a more secure and responsive approach to digital threats.

*****

DIGITAL SHADOW: SOCIAL MEDIA'S ROLE IN THE PROPAGATION AND PREVENTION OF REVENGE PORN IN INDIA

Lakshman Singh[144] and Neetigya Krishna[145]

ABSTRACT

This paper explores the intricately intertwined relationship these social media sites hold with the disturbing reality of revenge porn that hassles a country fast digitalizing its society-Country: India. In keeping with this understanding, we now examine the existing corpus juris by entering into an analysis of the Information Technology Act, 2000, along with amendments, specifically to Section 67A so as to criminalize obscene electronic publication. To this end, we scrutinize whether such provisions are adequate in dealing with challenges unique to non-consensual image sharing, firstly in light of the path-breaking judgment by the Supreme Court of Puttaswamy v. Union of India (2017), where the right to privacy is recognized as a fundamental right. In addition, we look into how the social media sites amplify the problem and then reduce it. Such ease of access, rampant usage, & viral nature of the sites make it easy for intimate images to be shared without one's consent, thereby inflicting irreparable damage upon victims. We take note of the policies and practices pursued by the major social media companies operating in India, subjecting them to a critical analysis of the effectiveness with which they respond to reports of revenge porn & delete the content. The article also discusses the social media as an empowered tool for victims in India. Here, we discuss online communities and advocacy groups that are on social media to raise awareness and try to offer legal aid and other things to survivors. Ultimately, the paper calls for an integrated approach wherein the strengthened legal framework is supplemented with enhanced platform accountability and robust victim support mechanisms toward effectively tackling the issue of revenge porn and more meaningfully protecting the digital rights of individuals in India.

Keywords: Revenge Porn, Social Media, India, Information Technology Act, Right to Privacy, Victim Empowerment.

INTRODUCTION

Unconsensual photo sharing, or revenge porn, involves posting sexually explicit images or videos of someone without their consent to embarrass or damage them. The rapid proliferation of social media as a form of self-expression and contact has made this a bigger problem in India (Deb, 2020). Digital revolution has revolutionised how individuals communicate and share information, resulting in exponential internet penetration in India. Social media has made personal data simple to exploit, putting users at risk. India's private and public use of social media is expanding as the country becomes more digital. Social media has become a double-edged sword since it may promote positive and harmful change. It facilitates communication but also spreads hateful content like revenge porn (Miftha, 2024). Sharing personal information on social media is easy and fast, making it practically difficult to delete, increasing the impact. We must recognise the ugly fact that women are disproportionately victims of this type of abuse.

This study examines revenge porn and social media in India, focussing on social and legal responses. The Information Technology Act of 2000 addresses cybercrime, but revenge porn may be too

[144] Student at Shri Ramswaroop Memorial University, India.
[145] Student at Shri Ramswaroop Memorial University, India.

complicated. This study examines Section 67A (which makes it illegal to possess or distribute sexually explicit material online) and Puttaswamy v. Union of India (2017), which established the right to privacy as a human right. The study will examine whether current legal safeguards effectively protect people in today's digital world from revenge porn's damaging repercussions. This article examines Indian social media policy and laws. Social media is used to spread intimate content without consent and to raise awareness and empower victims. This essay will also discuss how advocacy groups and internet forums might help survivors receive justice and emotional support. For actual revenge porn protection in India, the research suggests a more comprehensive approach that addresses propagation and prevention through stronger legislation and platform accountability.

THE ROLE OF SOCIAL MEDIA IN THE PROPAGATION OF REVENGE PORN

Ease of Access and Virality

Social media has made it easier to remain in touch, but it has also enabled hazardous habits like revenge porn. Multiple built-in techniques on these sites allow easy sharing of non-consensual intimate photos. Thanks to speedy sharing, re-sharing, and anonymous uploading, such photos can go viral quickly (Arora, 2019). The interconnected structure of social media platforms and their global reach make it difficult to regulate image or video distribution after posting. Many people from different places can view and share it. WhatsApp, Instagram, Twitter, and Facebook spread revenge pornography. These platforms' community nature and simplicity of posting and distributing multimedia material encourage users to share content without contemplating the consequences. Private images uploaded on WhatsApp or Twitter can go viral without the owner's consent. Due to their vast user bases and viral content, victims are embarrassed and helpless when their private images and videos go public on these platforms.

The Role of Anonymity and Lack of Accountability

Social media anonymity promotes revenge porn. Anonymous profiles and phoney identities make it hard to identify damaging content creators. Anonymous offenders feel more comfortable conducting detrimental activities without repercussions, making it harder for law enforcement to identify and apprehend them. Social networking sites with weak verification processes make it easier for bad actors to create several accounts and continue their disruptive activities (Huber, 2023). Social media networks' delayed or nonexistent response to revenge porn charges has also been criticised. Even though most platforms have community guidelines and reporting mechanisms, victims often encounter delays or non-removal of information. Intimate content often goes viral before the site intervenes. Because these networks' regulations aren't always clear or enforced, responsibility is lacking. This inaction worsens victims' pain and encourages a culture where disseminating content without consent is not punished. Retaliation porn thrives in obscurity because platforms don't act soon enough, hurting victims.

LEGAL FRAMEWORK ADDRESSING REVENGE PORN IN INDIA

Analysis of the Information Technology Act, 2000

The Information Technology Act, 2000 governs cybercrime and e-commerce in India. Section 67A, one of its most crucial elements, regulates electronic distribution of sexually explicit content, making it a

powerful tool against revenge porn. This section punishes electronic publishing or transmission of sexually explicit material with fines and five-year prison sentences (Dunn, 2020). Due of its focus on obscene publications, Section 67A does not adequately handle non-consensual picture sharing issues, even though revenge porn cases sometimes use it. The IT Act was revised to improve its provisions in response to a rise in cybercrimes. Revenge porn cases are often ambiguous because the law does not target non-consensual photo sharing. Despite Section 67A's pornographic criminal measures, consent for personal photo sharing is unsettled. Revenge porn cases are problematic because they include unauthorised distribution of personal content, which violates privacy and dignity. While internet laws have strengthened, revenge porn regulations remain weak (Naicker, 2020).

Impact of *Puttaswamy v. Union of India* (2017)

The Supreme Court's landmark Puttaswamy v. Union of India (2017) ruling upheld privacy as a constitutional right. This verdict affirms the premise that sharing private pictures without agreement constitutes a privacy infringement, which has major implications for revenge porn cases. Revenge porn violates privacy and often causes emotional and psychological harm. The Puttaswamy verdict allows victims to restrict internet disclosure of sensitive information. This verdict permits courts to consider the illicit distribution of private material an invasion of privacy, strengthening the victim's case (Halder, 2022). Despite this progress, it is unclear how well revenge porn has implemented privacy as a fundamental right. Next, identify practical legal answers to non-consensual image sharing and turn this constitutional right into effective and efficient remedies.

Gaps and Challenges

Even though privacy is a right and the IT Act protects against revenge porn, there remain gaps in the law. The lack of non-consensual photo sharing laws is a major hurdle. Revenge porn involves obscenity, privacy violation, and permission, making the IT Act's obscene publication laws insufficient. Such cases can be difficult to prosecute. Victims often struggle to report revenge porn because law enforcement may not be trained to handle the technical aspects of such instances. Due of anonymity, social media criminals are harder to catch and prosecute. It is unclear who should be held accountable if social media corporations fail to stop hate speech or respond fast to victims. To stop revenge porn in the ever-changing digital ecology, stronger laws and enforcement are needed.

SOCIAL MEDIA PLATFORMS' RESPONSES TO REVENGE PORN

Platform Policies and Practices

Due to the worrying rise of revenge porn, some online businesses have tightened rules to make it tougher to transmit explicit photographs of private regions without consent. Facebook, Instagram, Twitter, and other platforms allow users to report and remove revenge porn. For instance, Facebook allows users to report explicit photos and uses advanced machine learning to prevent re-uploads of flagged content to stop the spread of explicit images. Users can report unauthorised uploads on Facebook and Instagram (Rizzica, 2021). Users can report non-consensual photos under Twitter's "private information" policy, which prohibits sharing explicit media without consent. These services also use "hashing" technology to detect and block private photo uploads. This technology is being deployed with content review teams

to give victims a say in platform material. Major social media platforms have also worked with global organisations to build reporting procedures that connect revenge porn victims to counselling and legal services to help them cope with the emotional and psychological impacts of the content.

Effectiveness and Critique

Despite this, many believe social media's revenge porn responses are ineffective and inconsistent. Numerous victims have complained that platforms provide reporting tools, but removing harmful content takes hours or days. Even after reporting, victims find their private photos on other networks (Vitis, 2020). While hashing and similar technologies are beneficial, they are not perfect. Reuploads of infected material may pass through hashing systems and affect the victim. Some say platforms aren't clear enough about how they handle reported content. Users and platforms don't always communicate after a report, so victims don't know if the issue is being addressed. Lack of transparency and long reaction times may make victims doubt the platforms' privacy protections. These sites seldom prevent revenge porn, instead responding after the fact. Several case studies have shown social media platforms' revenge porn responses' pros and cons (George, 2024). For instance, in 2018, Facebook was criticised for banning graphic photo sharing in private groups despite doing little to stop it. However, platforms and law enforcement have collaborated to catch offenders and support victims. The overall opinion remains that platforms should improve their response systems, enforce laws more strictly, and take stronger preventive efforts to protect victims from revenge porn's devastating impacts.

SOCIAL MEDIA AS A TOOL FOR PREVENTION AND EMPOWERMENT

Awareness and Advocacy

Despite being a place for revenge porn, social media can prevent such crimes and give victims a voice. Online communities and advocacy groups have done a tremendous job highlighting revenge porn, warning against uploading photographs without consent, and connecting victims to resources (Rajagopal et al., 2021). Cyber Civil Rights Initiative and other Indian advocacy groups are using social media to increase awareness of revenge porn's psychological, emotional, and legal effects. By sharing personal stories, survivor guidance, and professional viewpoints, these networks humanise the issue and create crucial talks about improved protections. Through social networking, revenge porn victims can learn about their legal rights and how to pursue them. Many advocacy groups educate the public through online seminars and webinars on legal frameworks for non-consensual image sharing, such as IT Act applications. How to report improper social media content and use legal resources to protect personal data are also covered. These groups spread information about consent and digital safety on Facebook, Instagram, and Twitter, reaching a huge audience and maybe preventing revenge porn. Online organisations allow survivors to discuss their experiences, seek guidance, and connect with legal and emotional professionals (Ho et al., 2024). These groups foster solidarity by reassuring victims they are part of a community. Social media helps these various groups unite and advocate collectively by facilitating resistance and empowerment.

Victim Support Mechanisms

Social media now supports revenge porn victims in addition to public education. Internet counselling,

legal aid, and hotlines are available to victims. Multiple groups have teamed with social media companies to help victims access mental health professionals or legal aid. Facebook has worked with Indian groups to help revenge porn victims by giving tools to erase offending content and psychological and legal services (Rackley et al., 2021). Social media corporations, legal aid organisations, and mental health professionals must collaborate to create a support structure to address revenge porn's multifaceted effects. The digital ecosystem lets victims report content, obtain legal help, and get emotional counselling in one spot, speeding up recovery and justice. More victims are getting help via social media. Instagram and Facebook provide reporting and removal standards for non-consensual intimate photos and legal and mental health services. These social media technologies demonstrate that these platforms can combat revenge porn rather than enable it. However, these platforms must collaborate with advocacy groups and specialists to help victims quickly, thoroughly, and effectively. To empower victims, social media networks should be more proactive in stopping harmful content and giving timely relief.

THE NEED FOR AN INTEGRATED APPROACH

Strengthened Legal Framework

Despite its importance in prevention and support, social media needs a stronger legal framework. The Information Technology Act of 2000 and its modifications assist, but they won't address revenge porn in the digital age. Legal reform is needed to define non-consensual photo sharing and increase penalties for violators. India should implement revenge porn legislation like the UK or Australia to provide victims greater legal options. These legislative amendments should prioritise victim protection so revenge porn victims can seek justice without prejudice or reprisal (Aman Gautam et al., 2024). We need clearer internet data exchange standards, especially for social media. Clearer responsibilities for intermediaries to block dangerous information, stricter fines for platforms that don't comply, and faster content removal rules are needed. Legislation should prioritise data protection so platforms cannot misuse user data or violate privacy.

Platform Accountability

Social media sites must be held accountable for spreading revenge porn to combat it. Several sites' non-consensual content reporting and removal methods include vulnerabilities. People are questioning the platforms' commitment to efficiently resolving the issue due to sluggish response times, inconsistent material removal, and lack of transparency in user reports (Huber & Ward, 2024). Legislation and internal reforms can make platforms more accountable, which is crucial. Accountability can be improved by using AI and machine learning algorithms to detect and eliminate revenge porn content immediately after upload. These systems should work with humans to swiftly and accurately review flagged information. Platforms should be liable for removing dangerous information. Transparency metrics must be reported publicly. Establishing a framework for responsibility would ensure social media companies take their responsibilities seriously. Stronger rules should make social media platforms accountable for the time it takes to remove harmful content. Regulatory organisations may mandate platforms to remove non-consensual content and respond to user reports within defined times

or face penalties (Shreya & Dev, 2024). These initiatives would ensure that platforms aren't just responding to revenge porn but also preventing it through content control and management.

Comprehensive Victim Support

Any campaign to eradicate revenge porn should prioritise victim legal, psychological, and social support. Creating a victim support system and changing the legislation and platform responsibilities are needed to repair revenge porn's social and emotional damage. Victims should have access to mental health, legal, and community support. Governments, advocacy groups, and social media companies must collaborate to build this support structure to help victims immediately (Hoque et al., 2024). A cohesive system must provide victims with social support, psychological counselling, and legal aid. Centralised reporting and aid procedures from governments and social media firms can help victims get resources. Victims should also have access to low-cost or free advocacy groups and attorneys to help them navigate the court system and push for stronger legal protections. Society requires a strong support structure to help revenge porn victims recover and move on.

CONCLUSION

Social media anonymity and accessibility have made revenge porn popular, especially in India. Social media is amazing for its dual use. It uses virality and the lack of instantaneous responsibility to spread explicit, non-consensual content quickly. However, social media allows victims to express their ideas, raise awareness, and receive help, making it a potential weapon against this issue. Despite the Information Technology Act, 2000 and the Puttaswamy ruling, India's legal framework has severe gaps. Current laws fail to keep up with cybercrimes, leaving revenge porn victims without protection or retribution. The varied and slow responses of social media platforms to claims of non-consensual content make the issue worse, hence legislation and platform practices must be changed. A thorough plan is needed to combat revenge porn. Prioritise legislative reform. India must implement tighter laws to address non-consensual image sharing and punish perpetrators. Legislation should prioritise victim privacy and justice-seeking resources. People should also hold social media corporations more accountable for spreading revenge porn. This could be done by enforcing faster content removal timelines, being more transparent about report handling, and using automated methods to detect and halt problematic content. Finally, victim support must be strengthened. These include public awareness campaigns and legal and mental health services. Public education and lobbying must continue to make the internet safer. Awareness initiatives led by advocacy groups and supported by social media can shift public perception and reduce revenge porn. Victim support, platform responsibility, and legislative reform can reduce revenge porn in India more effectively.

REFERENCE

1. Deb, A. (2020). The Case for a New Statutory Regime Addressing Revenge Porn in India: Exploring the Disputed Terrain From a Feminist Perspective. *Available at SSRN 3884351*.
2. Miftha, A. (2024). The social, legal, and technical perspectives of cyberstalking in India.
3. Arora, P. (2019). *The next billion users: Digital life beyond the West*. Harvard University Press.

4. Huber, A. (2023). 'A shadow of me old self': The impact of image-based sexual abuse in a digital society. *International Review of Victimology*, *29*(2), 199-216.
5. Dunn, S. (2020). Technology-facilitated gender-based violence: An overview. *Suzie Dunn," Technology-Facilitated Gender-Based Violence: An Overview"(2020) Centre for International Governance Innovation: Supporting a Safer Internet Paper*, (1).
6. Naicker, P. (2020). *Exploring the understandings and experiences of cyber violence amongst teenage girls* (Doctoral dissertation).
7. Halder, S. (2022). Cyber Terrorism: A Threat to Human Society. *Jus Corpus LJ*, *3*, 175.
8. Rizzica, A. (2021). *Sexually explicit deepfakes: to what extent do legal responses protect the depicted persons?* (Doctoral dissertation, Master's Thesis Law and Technology. Tilburg Law School).
9. Vitis, L. (2020). Private, hidden and obscured: Image-based sexual abuse in Singapore. *Asian journal of criminology*, *15*(1), 25-43.
10. George, A. (2024). Defamation in the Time of Deepfakes. *Available at SSRN 4719803*.
11. Rajagopal, T., Chandrashekaran, V., & Ilango, V. (2023). Unmasking the Deepfake Infocalypse: Debunking Manufactured Misinformation with a Prototype Model in the AI Era "Seeing and hearing, no longer believing.". *Journal of Communication and Management*, *2*(04), 230-237.
12. Ho, M. H., Gupta, S., Lee, J., Wadhwa, B., & Fu, X. (2024). Detrimental to Our Digital Well-Being: Campus Sexual Misconduct and Technology-Facilitated Sexual Violence Among University Students in Singapore. *Violence Against Women*, 10778012241283498.
13. Rackley, E., McGlynn, C., Johnson, K., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). Seeking justice and redress for victim-survivors of image-based sexual abuse. *Feminist Legal Studies*, *29*(3), 293-322.
14. Aman Gautam, D. R. K. J., Narula, A., & Sharma, N. (2024). Mitigating Human Rights Violations Caused by Deepfake Technology. *Library Progress International*, *44*(3), 4628-4637.
15. Huber, A. R., & Ward, Z. (2024). Non-consensual intimate image distribution: Nature, removal, and implications for the Online Safety Act. *European Journal of Criminology*, 14773708241255821.
16. Shreya, & Dev, S. (2024). Sexual violence in cyberspace: breaking the silence of international law. *International Journal of Public Law and Policy*, *10*(4), 383-397.
17. Hoque, M. A., Ferdous, M. S., Khan, M., & Tarkoma, S. (2021). Real, forged or deep fake? Enabling the ground truth on the internet. *IEEE Access*, *9*, 160471-160484.

*****

ROLE OF POLICE IN INVESTIGATING DIGITAL CRIMES

Dr. Sunil Kumar[146]

ABSTRACT

As digital technology continues to permeate every aspect of modern society, the nature of threats in cyberspace is evolving dramatically. This paper explores the transition from cyber-terrorism to cyber warfare, highlighting the changing motivations, tactics, and implications for national security. Initially characterized by politically motivated attacks aimed at instilling fear or causing disruption, cyber-terrorism has increasingly intersected with state-sponsored activities, blurring the lines between non-state actors and nation-state aggressors. Examination of recent case studies illustrating this shift, including high-profile incidents that demonstrate the capabilities of state actors to conduct cyber operations that can achieve strategic objectives, disrupt critical infrastructure, and manipulate public perception. The implications of this evolution are profound, necessitating a re-evaluation of existing cybersecurity frameworks and defence strategies. This paper discusses the role of emerging technologies, such as artificial intelligence and machine learning, in shaping both offensive and defensive cyber capabilities. It emphasizes the importance of international collaboration and intelligence sharing to mitigate the risks posed by these evolving threats. By understanding the dynamics of this shift, policymakers and cybersecurity professionals can develop more effective responses to safeguard national interests in an increasingly interconnected and hostile digital landscape. This study ultimately calls for a holistic approach to cybersecurity that integrates technological innovation, legal frameworks, and cross-border cooperation to counter the complexities of contemporary cyber threats.

Keywords: Cyberterrorism, Cyber threats, Cybercrimes, Artificial Intelligence

INTRODUCTION

In today's interconnected world, digital crime, also known as cybercrime, has become a significant challenge for law enforcement agencies across the globe. The rapid advancement of technology has not only provided unprecedented opportunities for growth and development but also paved the way for criminals to exploit vulnerabilities in digital systems. Digital crime encompasses a wide array of offenses, including hacking, identity theft, cyberstalking, financial fraud, and even cyberterrorism. Given the complexities associated with such crimes, police forces are now required to adapt and enhance their investigative capacities to effectively combat the growing threat[147].

The role of the police in investigating digital crime has evolved significantly over the past two decades. Traditional crime-fighting techniques have proven inadequate in the face of highly technical cyber offenses, leading to the development of specialized units, cyber forensics, and international cooperation. This article explores the role of the police in investigating digital crime, examining the challenges they face, the techniques employed, and the legal frameworks that support this investigation.

WHAT IS CYBER CRIME?

Cyber crime refers to illegal activities that are carried out using computers, digital devices, or the internet. It encompasses a wide range of offenses, including hacking, identity theft, online fraud, cyber

[146] Assistant Professor of Law, Jagannath University, India.

[147] Lee, Y. H. (2020). How police policies and practices impact successful crime investigation: Factors that enable police departments to "clear" crimes. *Justice System Journal*, *41*(1), 37-62.

stalking, phishing, and the distribution of illegal content. Cyber criminals exploit vulnerabilities in computer systems, networks, and digital platforms to gain unauthorized access to sensitive data, disrupt services, or inflict damage on individuals, organizations, or governments. The anonymity offered by the internet, coupled with the global reach of digital networks, has made cyber crime a growing concern for law enforcement agencies worldwide[148].

The complexity of cyber crime lies in its often transnational nature, with perpetrators operating across different jurisdictions, making it difficult for local authorities to address such offenses effectively. Additionally, the tools used in cyber crime, such as encryption and malware, continually evolve, posing significant challenges for investigators. Law enforcement agencies, private sector entities, and international organizations are required to collaborate closely to develop effective strategies for combating cyber crime, which remains a major threat to personal, financial, and national security in the digital age[149].

TYPES OF CYBER CRIME

Cybercrime encompasses a broad range of illegal activities that target or exploit digital systems and networks. The primary types of cybercrime include[150]:

1. Hacking: Unauthorized access to computer systems or networks, often aimed at stealing or manipulating data, or disrupting services. This may also include the use of malware, such as viruses or trojans, to infiltrate systems.
2. Phishing: Fraudulent attempts to deceive individuals into providing sensitive information, such as login credentials or financial details, by posing as a legitimate entity through emails, messages, or websites.
3. Identity Theft: The unauthorized acquisition of personal information with the intent to impersonate an individual and commit fraud, such as opening bank accounts, securing loans, or making unauthorized purchases.
4. Ransomware Attacks: The deployment of malicious software that encrypts a victim's data, with the attacker demanding a ransom to restore access to the information.
5. Cyber stalking and Harassment: The use of digital platforms to harass, threaten, or stalk individuals, often causing emotional distress or fear.
6. Online Fraud: Various forms of deceptive practices, such as financial scams, auction fraud, or counterfeit product sales, conducted through digital platforms.

These cybercrimes pose significant risks to individuals, businesses, and governments, requiring coordinated efforts in digital forensics, cyber security, and international cooperation to mitigate their

[148] Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.
[149] Bjelland, H. F., & Dahl, J. Y. (2017). Exploring criminal investigation practices: The benefits of analysing police-generated investigation data.
[150] Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cyber crimes in India. In *2020 International conference on emerging smart computing and informatics (ESCI)* (pp. 269-275). IEEE.

impact.

CRITICAL VIEW OF CYBER CRIME AND CYBER POLICING

In the fast-paced, ever-changing world that characterizes the fields of cyber policing and cybercrime investigation, there are an abundance of challenges and obstacles that need to be overcome, as was previously said. These have been discussed in the following ways[151]:

Legal Framework:

The most critical issue in cyber policing and investigation of cybercrime is the legal framework within which it operates. Before the Information Technology (IT) Act, 2000 was passed, the cyber world within the context of India remained unregulated, and there was an element of doubt among the law enforcing authorities regarding the acceptable course of action to be followed in response to criminal offenses that were committed in cyberspace. The legislative initiative that gave rise to the creation of the IT Act, 2000 helped to define cyber crime and make cyber policing and investigation a practical possibility for the first time. Besides, since the Act is dynamic, it was felt that some provisions required updating. What's more, meeting the ends of the Act remained to be incorporated in the year 2008. This placed powers to inquire into cyber offenses in the hands of an Inspector instead of the Deputy Superintendent of Police that was granted by the existing legislation. This Act also encompasses further forms of illegal action that could be performed online, including cyber terrorism and child pornography[152]. As a result of this, the legal framework seeks to answer a range of questions, one of which is the following:

What type of investigation will be conducted on that computer crime? What type of consequences might an individual end up if they are caught committing such a cyber crime? In the context of the internet, what is "evidence"?

Cyber Crime Investigation:

Section 78 of the IT Act deals with the investigation of cyber crimes. Section 80 of the Act grants the rights of entry and search, and other similar rights to police officers and other officers. With the rise of even more dangerous cyber crimes, one would logically anticipate a corresponding rise in those who are determined to be convicted of such crimes[153].

This has not always has not been the case, however, as reflected by the fact that thousands of investigations and prosecutions have been lagging behind. Brown (2015) holds the opinion that some of the primary reasons behind this outcome are trans-jurisdictional barriers, dishonesty, and incapacity of major actors in the criminal justice systems to understand the basic aspects of technology-assisted crime. Most jurisdictions have only one or a very few police stations which dedicated to investigating cybercrime, which may not be sufficient enough to keep up with the exponential rise in the number of

[151] Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, *19*(6), 519-536.
[152] Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cyber crimes in India. In *2020 International conference on emerging smart computing and informatics (ESCI)* (pp. 269-275). IEEE.
[153] Katos, V., & Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces*, *30*(4), 223-228.

crimes that are committed online. Furthermore, it is daunting for victims to reach a specific police station in order to file complaints (Kaumudi, 2016)[154].

The crucial challenges faced in cyber crime investigation are :

- Lack of trained cyber investigators.
- Very few cyber forensic facilities are available in Forensic Labs.
- Massive pile-up of reports not received till date.
- No institutional mechanism is there to seek the help from cyber experts at the industrial level.

Supreme Court Judgment of 2006 & Model Police Act:

According to the judgment rendered by Supreme Court of India on September 22, 2006 in the case of Prakash Singh and Others vs. Union of India and Others, there was also a directive forming the judgment which stated, "The investigating police shall be separated from the law and order police to ensure faster investigation, better expertise, and improved rapport with the public.". The directive stated that this separation was necessary to assure these things. However, complete coordination between both wings is something that has to be achieved. This fact has been further brought out in the Model Police Act of 2006, which was enacted in 2006. Apart from this, several state legislatures have enacted resolutions that are similar to these acts. It is not a task that could be referred to as routine while taking into consideration the current state of the criminal environment; people must receive special training and policing and investigation of cyber crime is not something that can be dealt with within routine or by anyone. The personnel have to be chosen very carefully, trained, and given sufficient time to master their skills over a period of years.

Collaboration between Police and Administrative Agencies in Cyber Crimes:

Indian cyber crimes investigation is all about teamwork. Police and administrative authorities have to reenact their buddy cop to bust those cyber culprits. This means efficient

communication, joint task forces, and a sharing of a common mission, which is to protect the digital world. In the land of cybercrime, sharing is indeed caring. Information is the key to unlock mysteries regarding cyber offenses. Police and administrative agencies will have to exchange data even faster than children trade Pokémon cards. Effective information-sharing protocols can make them stay ahead of all the cyber baddies[155].

EMERGING CRIMES IN CYBER CRIME INVESTIGATION IN INDIA

As India accelerates its adoption of digital technologies, the scope of cyber crime also transforms. With increasing dependence on these platforms for banking, commerce, communication, and governance,

[154] Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1-22.
[155] Anwary, I. (2023). Evaluating Legal Frameworks for Cybercrime in Indonesian Public Administration: An Interdisciplinary Approach. *International Journal of Cyber Criminology*, *17*(1), 12-22.

cyber criminals have found ways to exploit these platforms. Some of the emerging cyber crimes in India, as of October 2023, are[156]:

Ransomware Attacks:

Definition: Ransomware is malicious software that encrypts a victim's data and renders it inaccessible unless a ransom is paid, typically in cryptocurrencies.

Emergence in India: Hackers are targeting Indian organizations, and vulnerabilities in the security systems are being exploited. It has caused critical operational disruptions and financial losses.

Phishing and Smishing Scams:

Phishing: It refers to deception through e-mails where fraudsters obtain personal information from the user. Smishing is a similar fraud that uses SMS messages. Emerge in India: With millions accessing the Internet using mobile devices, the fraudsters use bank or government institution's identity to extract passwords and all other financial information.

UPI Frauds:

Uplines Description: UPI enables instant money transfers between bank accounts through mobile devices.

Emergence in India: The fraudsters take advantage of innocent users who are not aware of the features of UPI. It sends a fake payment request or codes and sends money when authorized from the victim's account.

Cyber stalking and Online Harassment:

Description: Harassment or stalking through digital media.

Rise in India: It has progressed along with the mushrooming of social media and largely affects women and children. Cyberstalkers can blackmail or threaten with the help of personal information.

Deep-fakes and Synthetic Media:

Description: Deep-fakes, basically AI-generated pictures or videos, are perceived as true.

Emergence in India: These technologies are being used to create fake content by spreading misinformation, defamation, or even fraud[157].

Cryptocurrency-Related Crimes:

Description: Crimes made using digital currency, including Bitcoin.

Emergence in India: Fake investment schemes, unauthorized mining, and use of cryptocurrencies for money laundering because of their semi-anonymous nature[158].

---

[156] Gupta, T. (2023). EMERGING TRENDS OF CYBER CRIME IN INDIA: A CONTEMPORARY REVIEW. *Journal of Law and Policy Transformation*, *8*(1), 57-65.

[157] Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE access*, *10*, 25494-25513.

[158] Maurushat, A., & Halpin, D. (2022). Investigation of cryptocurrency enabled and dependent crimes. In *Financial Technology and the Law: Combating Financial Crime* (pp. 235-267). Cham: Springer International Publishing.

Internet of Things (IoT) Vulnerabilities:

Description: IoT devices comprise any internet-connected devices like smart home appliances.

Emergence in India: Poor security in IoT devices allows hackers to create botnets or gain unauthorized access to personal networks, leading to data breaches.

Cyber Espionage:

Description: Unauthorized access to confidential information for strategic or competitive advantage.

Emergence in India: It includes government agencies and companies where attackers are searching for sensitive data on national security or intellectual property.

Child Exploitation and Abuse Material (CEAM):

Description: The production, distribution, or possession of child sexual abuse material.

Surge in India: The anonymity of the internet enables CEAM proliferation, which further complicates law enforcement efforts to identify and prosecute these perpetrators[159].

Financial Frauds and Investment Scams:

Description: Cons involve deceiving people into putting their money in investments with false promises.

Surge in India: Online platforms are used to circulate Ponzi schemes, fake stock tips, or other investment scams that promise supposed high returns.

Dark Web Activities:

Definition: Illegal activities conducted on the dark web, that portion of the Internet which is not indexed by typical internet search engines.

Emergence in India: This has included exchanging contraband, hacking software, and stolen data. Indian users are increasingly both victims and offenders in dark web transactions[160].

Malware and Spyware:

Definitions: Malicious programs designed to harm or gain unauthorized access to systems.

Emergence in India: Attackers use malware associated with an infected attachment to an email, compromised website used by attackers or downloading otherwise free or pirated software to collect data or track user activity.

CHALLENGES IN INVESTIGATING EMERGING CYBER CRIMES IN INDIA

Investigating emerging cybercrimes in India poses a complex set of challenges for law enforcement agencies, the police, policymakers, and the judiciary. The sophistication of the cybercrime fraternity coupled with the worldwide and decentralized nature of the internet makes the detection, investigation,

[159] Cream, J. (1993). Child sexual abuse and the symbolic geographies of Cleveland. *Environment and Planning D: Society and Space*, *11*(2), 231-246.
[160] He, S., He, Y., & Li, M. (2019, March). Classification of illegal activities on the dark web. In *Proceedings of the 2nd international conference on information science and systems* (pp. 73-78).

and subsequently, prosecution of such offenses complex. Some of the most prominent challenges include[161]:

Lack of adequate technical expertise -

Challenge: Cybercrimes are highly sophisticatedly cyber-based with technical methods like encryption, blockchain, and anonymization methods such as VPN the Dark Web. In India, there might be a scarcity of personnel with special technical skills to investigate crimes.

Impact: The lack of cyber forensic experts and trained personnel bars effective analysis of digital evidence as well as tracing the culprit.

Jurisdictional Issues and Cross-Border Nature of Cybercrimes -

Challenge: Cyber prosecutions for crimes in many countries across borders where hackers are beyond Indian borders using servers from other countries. It is difficult to identify whose jurisdiction prevails[162].

Impact: International cooperation is delayed due to legal and bureaucratic red tape, thereby making it arduous to track and apprehend such offenders who make use of jurisdictional openings.

Anonymity of Cyber criminals -

Challenge: Cybercrime allows criminals to mask their identities as better usage encryption, proxy, and dark web make it difficult for them to trace.

Impact: In such cases, tracing his physical movements or even the digital footprints may go out of hands of an observer using traditional methods of an investigation, meaning that the prosecution may fail to proceed or can be delayed since the accused cannot be traced due to lack of vigilance[163].

Inadequate Existence of a Holistic Legal Framework -

Challenge: Although Indian law has enactments like the Information Technology Act of 2000, the ongoing advancements in cybercrimes involving cryptocurrency and deepfakes cannot be kept in pace by the same.

Impact: Loopholes created by this existing framework create challenges in some cases of cybercrime, especially those utilizing very advanced technologies like deep fakes or cryptocurrency.

Slow Judicial Process -

Challenge: The Indian judicial system suffers from delayed processes, the underutilization of technology in courts, and procedural delays in handling cybercrime cases.

Impact: Such delays can cause cases to become long-drawn affairs, dilute the punishments, and allow cyber-criminals to gain the lead against law enforcement.

Handling and Preserving Digital Evidence -

[161] Dhupdale, V. Y. (2010). Cyber Crimes in India and the Challenges Ahead. *Indian JL & Just.*, *1*, 102.
[162] Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*.
[163] Lusthaus, J. (2016). *Cybercrime: The industry of anonymity* (Doctoral dissertation, University of Oxford).

Challenge: "The collection, preservation, and presentation of electronic data are technically complex because such data are by nature volatile.".

Impact: The case against the offender is compromised in court because of the increased likelihood that data corruption or loss will occur in the absence of standard processes and infrastructure for managing digital evidence[164].

Privacy and Encryption -

Issue: A right to privacy combined with encryption for protecting individual data are what stand in the way of investigators, since they would only gain access to encrypted communication, should they find a suitable balance between privacy rights and safety in public.

Impact: Investigators may be legally restrained from accessing encrypted data, particularly with end-to-end encryption becoming more prevalent in messaging services such as Whatsapp, which would slow an investigation.

Under-reporting of Cybercrimes -

Challenge: Most cybercrimes, especially financial fraud and harassment cases, are underreported because of a lack of awareness, stigma, or fear about damage to the reputation.

Impact: Under reporting limits the ability of the law enforcement agencies to assess the extent of the problem that is at hand, and it also diminishes the chances of building strong cases based on numbers of victims[165].

Lack of Public Awareness and Cyber Hygiene -

Challenge: Massive population in India is not well-versed about basic practices in cyber security, making them vulnerable prey to phishing attacks and social engineering, and glaring vulnerabilities in UPI fraud[166].

Impact: Public unawareness has become a colossal pool of victims, as the scenario is well-overwhelming the law enforcing agencies and making all the Preventive measures ineffective.

Interagency and International Coordination –

Challenge: To probe cybercrime, often multiple agencies from the internal (such as CERT-In, NIA, and CBI) and external (such as Interpol, other nations' agencies on cybersecurity etc.) are required to be coordinated.

Impact: The overall investigation may be delayed or complicated because the agencies do not coordinate with each other properly. Even international cooperation typically is sluggish, at least when MLATs are absent[167].

---

[164] Granja, F. M., & Rafael, G. D. R. (2015, July). Preservation of digital evidence: application in criminal investigation. In *2015 Science and Information Conference (SAI)* (pp. 1284-1292). IEEE.
[165] Sangari, S., Dallal, E., & Whitman, M. (2022). Modeling under-reporting in cyber incidents. *Risks*, *10*(11), 200.
[166] Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36-45.
[167] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. *Applied Sciences*, *13*(6), 3410.

Rapid Technological Change and Evolving Cybercrime Techniques -

Challenge: Rapid progress in technology makes it very difficult for the law enforcement to innovate and respond in the right time through different types of cybercrimes, which may include AI-driven phishing, quantum cryptography, and machine learning-based malware.

Impact: Law enforcement can't keep pace in developing their ability to predict and counter new cyber threats before these are quickly adopted by cyber crime practitioners[168].

Resource Constraints -

Challenge: Indian police face budgetary and resource constraints within most the smaller towns or villages; absence of appropriate funding to set up cyber forensic labs, advanced versions of software tools, or acquire expert training.

Impact: Cybercrime investigations in under-resourced areas will probably be over delayed or inadequately handled, therefore enabling cyber criminals to escape justice[169].

CONCLUSION

Police forces are now the only authority to be looked at as investigating Cyber crime because the speed at which the nation of India is transforming into a digitally advanced country. The numerous types of cyber threats that can even range from monetary fraud and cyber-stalking, data breach, pose distinct challenges for law enforcement agencies in tracking and prosecution. Crime- solver police have had to keep pace with rapid changes in the technological environment. Despite limited resource availability, skill gaps in technology, and jurisdictional complications, police remain at the forefront of protection of citizens and businesses from online threats. The development of technological capacities could provide advantages to police in combating cyber crime more effectively because of improved inter-agency collaboration and the inculcation of awareness among the public. But continued efforts to upgrade cyber laws, training, and infrastructure will be required to equip the law enforcement agencies as India confronts the looming digital threats. The police always have to adapt and evolve ahead of the cyber criminals they are to apprehend to bring justice in this highly virtual world.

In conclusion, it can be stated that cyber policing and cyber crime investigation call for a higher level of professionalism than ever before, as well as the ability to remain stealthy, make use of automated technologies, and understand the complexities of the online world.

*****

[168] Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. *Computer Fraud & Security, 2019*(6), 8-11.
[169] Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019, June). Measuring the changing cost of cybercrime. In *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*.

"Cyber Security and Artificial Intelligence: Emerging Trends" explores the critical intersection of two transformative fields shaping the modern digital era. This edited volume compiles 48 meticulously researched papers that delve into the challenges, opportunities, and innovative solutions in cyber security and artificial intelligence. Covering a wide range of topics such as ethical considerations, legal frameworks, policy implications, and technological advancements, this book is an indispensable resource for students, academics, researchers, and practitioners.

Curated from the National Conference on Cyber Security and Artificial Intelligence, this book reflects the collaborative efforts of distinguished scholars and experts in the field, offering insights that are both theoretical and practical.

Editorial Board:

1. **Dr. Ausaf Ahmad Malik** *[Principal and Professor, School of Law, Rai University, Ahmedabad]*
2. **Mr. Abhilash Aggarwal** *[Head of Department, School of Law, Rai University, Ahmedabad]*
3. **Adv. Gyan Prakash Kesharwani** *[Advocate & Chairperson, VidhiAagaz]*
4. **Mr. Dinesh Kumar Mishra** *[Assistant Professor. School of Law, Rai University, Ahmedabad]*
5. **Ms. Prachi Tripathi** *[Assistant Professor. School of Law, Rai University, Ahmedabad]*
6. **Adv. Aishwarya Gupta** *[Advocate & Editorial Head, CLRS, VidhiAagaz]*

Published By: *VidhiAagaz in collaboration with School of Law, Rai University, Ahmedabad, India.*

Rai University
EVO'V'NG THINK NG MINDS

Web: https://www.raiuniversity.edu/

www.vidhiaagaz.com

VidhiAagaz
Inking Your Brain

Maihar,
Madhya Pradesh.

First Impression:
2024

ISBN 978-81-947620-5-8