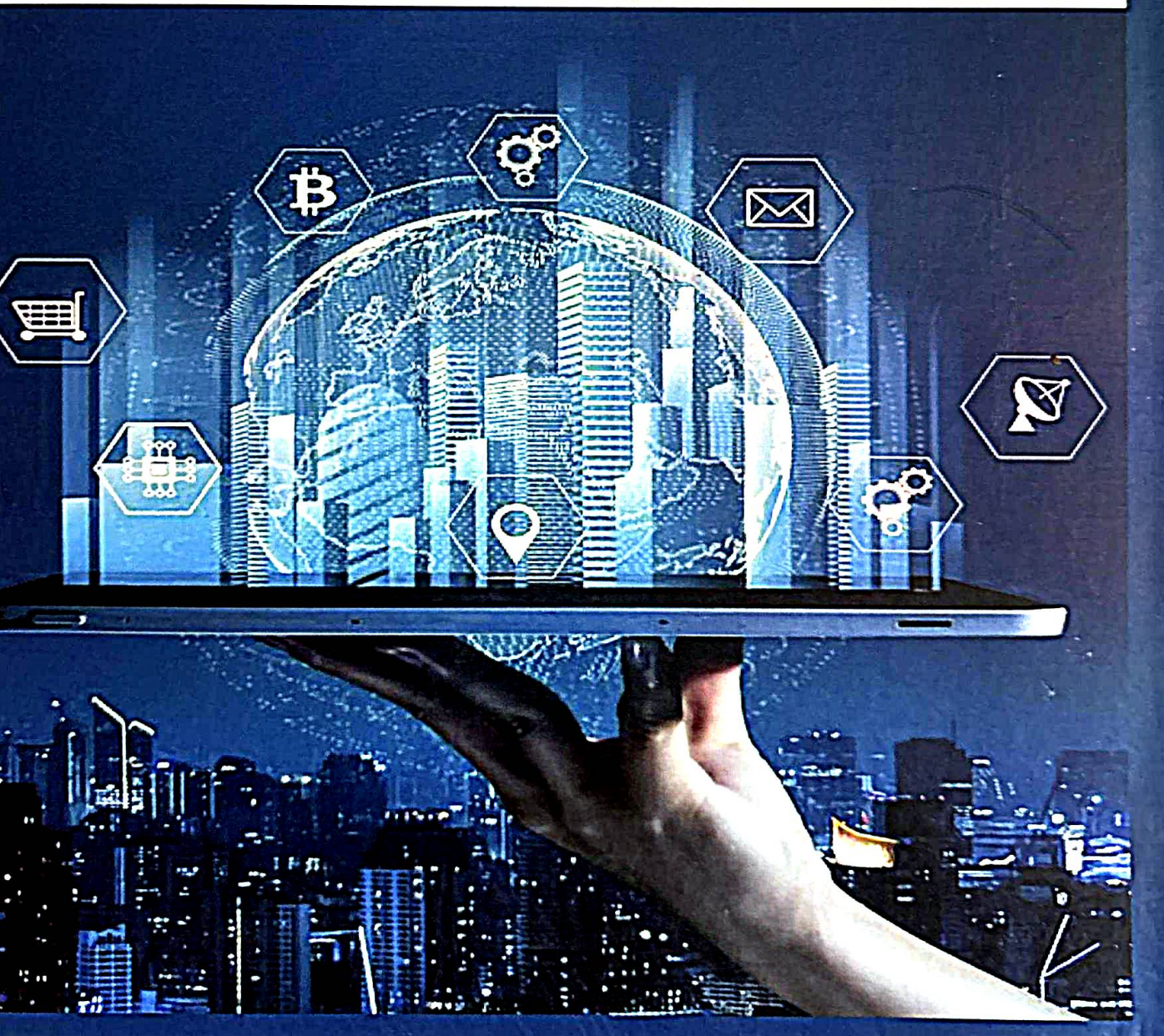
Artificial Intelligence and Data Privacy

Balancing Innovation and Security in the Digital Age

Dr. Anjali Dixit



Artificial Intelligence and Data Privacy

Balancing Innovation and Security in the Digital Age

Edited by

Dr. Anjali Dixit
Sr. Associate Professor of Law,
SOL, Lingaya's Vidyapeeth
(Deemed to be University), Faridabad, Haryana,
Visiting Professor, Department of Law
KAAF University College
Gomoa Fetteh, Kakraba-Kasoa,
Ghana (West Africa)

ABS Books
Delhi-110086

The responsibility for facts stated, opinion expressed or conclusions reached and plagiarism, if any, in this book is entirely that of the author(s). Neither the publisher nor the editors will be responsible for them whatever.

ISBN : 978-81-19708-34-5

Copyright : Editors

Edition : 2025

Published by

ABS Books

Publisher and Exporter

B-21, Ved and Shiv Colony, Budh Vihar
Phase-2, Delhi - 110086
✆ : + 919999868875, +919999862475
✉ : absbooksindia@gmail.com

Website : www.absbooksindia.com

PRINTED AT

Trident Enterprises, Noida (UP)

Overseas Branches

ABS Books

Publisher and Exporter

Yucai Garden, Yuhua Yuxiu
Community, Chenggong District,
Kunming City, Yunnan Province
-650500
China

ABS Books

Publisher and Exporter

Microregion Alamedin-1
59-10 Bishek, Kyrgyz
Republic- 720083
kyrgyzstan

Artificial Intelligence and Data Privacy: Balancing Innovation and Security in the Digital Age

By : *Dr. Anjali Dixit*

Preface

In the dawn of the digital age, the interplay between artificial intelligence (AI) and data privacy has emerged as one of the most pressing issues of our time. As technology advances at an unprecedented pace, the challenge of balancing innovation with security has become a critical concern for policymakers, legal scholars, and the global community. The book ***Artificial Intelligence and Data Privacy: Balancing Innovation and Security in the Digital Age*** delves into this complex and multifaceted relationship, offering a comprehensive exploration of the legal, ethical, and practical dimensions of AI and data privacy.

This volume brings together contributions from a distinguished group of scholars and practitioners who provide valuable insights into various aspects of AI and data privacy. **Dr. Anjali Dixit**, Senior Associate Professor of Law at Lingaya's Vidyapeeth and Visiting Professor at KAAF University College, starts the discussion with her chapter on *AI, Machine Learning & Big Data Laws and Regulations 2024*. Her work offers a critical analysis of the evolving legal landscape surrounding AI and data privacy.

Professor (Dr.) Rohit P. Shabran, Director of the Institute of Legal Studies at Shri Ramswaroop Memorial University, addresses *Data Privacy vs. AI Innovation: India's Balancing Act*. His examination highlights the delicate equilibrium that India seeks to achieve between fostering technological innovation and safeguarding data privacy.

B Mathanachandiran and **Dr. Ratheesh Kumar V.V** from VISTAS, Chennai, explore the interplay of *Artificial Intelligence, Data Governance & Privacy*. Their insights contribute to a deeper understanding of how AI is reshaping data governance and privacy frameworks.

Dr. Madhuri Vijay Sarwade, Associate Professor at Tilak Maharashtra Vidyapeeth's Lokmanya Tilak Law College, presents her research on *Emerging Patterns in Cybercrime Affecting Online Transactions and Banking Frauds in India*. Her work sheds light on the growing challenges of cybercrime in the digital age.

Dr. Sangeeta Sharma examines *AI & Law and Its Role in Future Legal Practice*, providing a forward-looking perspective on how AI might influence legal practices and the legal profession.

Aparna Chandra and **Sonal Rao**, Ph.D. scholars, delve into the *Evolution and Challenges of Data Protection Laws in India: A Critical Analysis*. Their contributions provide a critical assessment of the development and challenges of data protection laws in the Indian context.

Prof. (Dr.) Aqueeda Khan investigates *Artificial Intelligence in the Criminal Justice System*, offering insights into how AI technologies are being integrated into criminal justice practices and their implications for fairness and efficiency.

Dr. Anita Yadav discusses *Digitalization as a Concern of Privacy: Emerging Issues and Legal Framework*, highlighting the evolving concerns related to digitalization and the corresponding legal responses.

Mrs. R. Vimala and **Shahana Parveen P P**, along with **Dr. Mahesh M M**, explore the implications of *Digital Consumer's Confidentiality* and the impacts of excessive digital device use, respectively. Their chapters emphasize the significance of maintaining consumer confidentiality and addressing the psychological effects of digital overuse.

Dr. Devyani Chatterji and **Dr. Sapna Saxena** provide perspectives on *Indian Government's Policies on Cyber Security* and *Globalization and New Trends of Crime*, offering a comprehensive view of the policy landscape and emerging global crime trends.

Ms. Neha Prajapati and **Dr. Gunjan Baheti**, along with **Ms. Vinit Raikwar**, address the *Difficulties of Protecting Individual Rights in Artificial Intelligence* and explore the intersection of AI and legal practice in banking and financial sectors.

Finally, **Dr. Aneesh V Pillai** and **Nandana Rajesh** contribute a chapter on *Privacy and Data Protection: A Human Rights Perspective*, emphasizing the fundamental human rights dimensions of data protection in the context of AI.

This book aims to foster a nuanced understanding of how AI technologies intersect with data privacy and to provide practical insights into creating a balanced approach that promotes innovation while ensuring robust security and privacy protections. We hope this volume serves as a valuable resource for academics, practitioners, policymakers, and anyone interested in navigating the complex terrain of artificial intelligence and data privacy in the digital age.

Contents

Preface *v*

1. **Artificial Intelligence, Machine Learning & Big Data Laws and Regulations 2024** 1
   Dr. Anjali Dixit
2. **Data Privacy vs. Artificial Intelligence Innovation: India's Balancing Act** 17
   Prof. (Dr.) Rohit P. Sabran
3. **Artificial Intelligence, Data Governance & Privacy-An Analysis** 23
   Mr. B Mathanachandiran & Dr. Ratheesh Kumar
4. **Emerging Patterns in Cyber Crime Affecting Online Transactions and Banking Frauds in India** 40
   Dr. Madhuri V. Sarwade
5. **Artificial Intelligence & Law and its Role in Future Legal Practice** 55
   Dr. Sangeeta Sharma
6. **Evolution and Challenges of Data Protection Laws in India : A Critical Analysis** 59
   Ms. Aparna Chandra
7. **Artificial Intelligence in Criminal Justice System** 76
   Ms. Sonal Rao & Prof. Dr. Aqueeda Khan
8. **Digitalisation A Concern of Privacy: Emerging Issues and Legal Framework** 85
   Dr. Anita Yadav

9. **Digital Consumer's Confidentiality and Artificial Intelligence: An Analysis** 102
Mrs. R. Vimala

10. **Impacts of Excessive Digital Device Use** 118
Ms. Shahana Parveen P P & Dr. Mahesh MM

11. **A Comprehensive Study of Indian Data Protection Laws** 130
Ms. S. Syed Ali Fathima Nisha & Mr. Vijay. M

12. **Indian Government's Policies on Cyber Security** 139
Dr. Devyani Chatterji

13. **Globalisation and New Trends of Crime : An Overview** 150
Dr. Sapna Saxena

14. **Difficulties of Protecting Individual Rights in Artificial Intelligence** 160
Ms. M. Mahisha Malar & Mr. Selgin. B

15. **The Intersection of Artificial Intelligence and Legal Practice: Exploring the Future of Legal Services in Banking and Financial Sectors** 172
Ms. Neha Prajapati & Mr. Vinit Raikwar

16. **Privacy and Data Protection: A Human Rights Perspective** 189
Dr. Aneesh V Pillai & Mr. Nandana Rajesh

17. **Role of Social Media in Shaping Public Opinion in the Age of AI: An Indian Perspective** 199
Mr. Ramnik Bali & Ms. Arushi Khajuria

18. **Social Media Surveillance and Employment: Legal Issues in Monitoring Employee Behaviour** 204
Ms. Poorvaja G, Ms. Shravit Arora & Ms. Mini Srivastava

19. **Taming the Giant – Analyzing the Potential Possibilities of Inclusion of Artificial Intelligence in the Judiciary** 214
Ms. A. Anchirppa

Index 222

4.

Emerging Patterns in Cyber Crime Affecting Online Transactions and Banking Frauds in India

*Dr. Madhuri V. Sarwade**

Introduction

With the increase in internet, the whole world has become a global village wherein everything is easily accessible. Technology has made international communications and interaction easier and quicker. A business in Tokyo can find a supplier in Mexico City trough a quick series of searches on the internet. An agreement might be stuck in a short period of time through the exchange of order forms through e-mail communications. Travelling might not be necessary at all. This has lead to an increase in the number of internet transactions[1]. Considering the current situation and circumstances internet has become an indispensable part of our daily lives.[2]

1. Indian Bar Review. Vol. XLI (2) 2014.p.181-182.
2. Ibid 182.

*Associate Professor in Tilak Maharashtra Vidyapeeth's Lokmanya Tilak Law College, Mukundnagar, Gultekdi, Pune, Maharashtra.

"Google knows quite a lot about all of us. No one ever lies to a search engine. I used to say that Google knows more about me than my wife does, but that doesn't go far enough. Google knows me even better because Google has perfect memory in a way that people don't".

– Bruce Schneier, Cyber Security Expert[3].

With the technological advancement almost all the information is now being stored in electronic media. Easy storage features and the reduced cost of storage media have created paperless offices, which are more efficient in discharging their functions. Computer technologies also have proliferated into the economic sectors (Banking and Insurance), social sectors (police help- lines, Academic and scientific research) health and other agencies[4].

India's Digital Banking Landscape

The banking industry has enjoyed the ride of emerging technology to undergo significant changes. Banks are among the biggest beneficiaries of the IT revolution and have largely adopted IT solutions for rendering the banking services to their customers[5]. The latest development of IT[6] and electronic media has emerged as one of the most prominent technology which has revolutionary effect on people's life all along the world. Inventions, discoveries and technologies widen the scientific horizons but also pose new challenges for legal world. IT brought about by computers; internet and cyber space has also posed new problems in jurisprudence. But there has been widespread growth of these crimes today and has become a matter of global concerns and pose a serious challenge for law enforcement agencies in the new millennium. These crimes are so peculiar that it can be committed anonymously far away from the victim without being physically present there.[7] Cyber criminals have also a cutting edge and a major advantage because they can use the computer technology to a nicely and inflict damage without any risk of being caught.

Crimes today is an international problem and has no national boundaries and cyber terrorists can even collapse the economic structure

3.Indian Bar Review, Vol. 46 (1) 2019 p.107.
4. Ibid 109.
5. "Cyber-Crimes: A Growing Threat to Indian Banking Sector", By Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru http://www.ijetsr.com/images/short_pdf/1516556483_926-933-SJ99_SIMRAN.pdf
6. Britannica Concise Encyclopedia defines 'technology' as the application of knowledge to the practical aims of human life. http://www.answers.com/library
7. An Introduction to Cyber Laws, "By J.P. Mishra, Central Law Publications, First Edition., 2012

of a country. It is cyber-attack which has grown in gigantic proportion and has become a top threat so the fear of cyber insecurity is today the topmost threat, while terrorist attack has become second.

Unfortunately, cybercrime is a growing problem in developing countries, where customers often conduct financial transactions over unsecure mobile phones and transmission lines that are not designed to protect communications[8]. Moreover cyber-crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. Further complicating cyber-crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself efficiently enact laws that comprehensively address the problem of the internet crimes without cooperation from other nations. While the major international organizations like the OECD and G-8 are the seriously discussing co-operative schemes, but many countries do not share the urgency to combat cyber-crimes for many reasons. Though the issue of jurisdiction in cyber space cannot be settled spontaneously, but still a global effort in this direction is the need of hour. [9]

Complexities Arising from Cyber-Crimes and Internet Exploitation

The most dangerous frauds that causes in day to day banking activity is phishing, a criminal activity using social engineering techniques [10].Cyber space does not recognize geographical boundaries. This has proved boom to the delinquents who perform illegal activities on the internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the part of law enforcement agencies further complicates the matter.[11] The challenges posed by cyber-crimes can be categorized into three main areas:

- **Legal Challenges:** These arise from the need for effective statutory provisions that can be utilized as tools for investigating and controlling cyber-crimes.
- **Operational Challenges:** These demand the presence of a well-trained and well-equipped investigative force that can operate

8. "4 Cyber Attacks that Threaten Financial Inclusion"By Silvia Baur-Yazbeck Available at: https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion. Last seen on 18/03/2020. 1.31pm.
9. Indian Bar Review, Vol XL (2) 2013.
10. "A Critical Analysis of Cyber Phishing and its Impact"., by S. Kumudha and Aswathy Rajan https://acadpubl.eu/hub/2018-119-17/2/128.pdf dated 17/03/2020. 11.02am.
11. Dr Amita Verma's, "cyber-crimes and Law"- Central Law Publications, 1st edition 2009, p.55.

and coordinate efficiently at both national and international levels.

- **Technical Challenges:** These involve obstacles that hinder the ability of law enforcement agencies to track down and prosecute offenders operating in the digital realm.

The Expanding Threat of the Internet Menace

Nobody had anticipated that one day development of internet, a great opportunity of communication and data transfer could also become curse for the mankind in a number of ways and internet could be misused for criminal activities.

Cyber-crime is a matter of great concern in today's networked world.[12]

Financial Impact of Cyber Crime on Banks

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions [13]. To appreciate the extent and scope of the menace of cyber, there is need to elaborate various types of cyber crimes.

- **Unauthorized Access:** Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system. To elaborate, we are living in a modern world. We would prefer our children use internet, but at the same we are watching, amount of time spend by them no doubt it is helping but negative never should overcome how to balance is our job.[14]

Hacking[15]

Hacking means unauthorized access to computers. Those individuals engaged in hacking activities have been termed hacker[16]. Hacking is very broad term.[17] No computer system in the world is completely protected from hacking and every system in the world can

12. Ibid
13. "International Research of Journal and Academic Review., "The effect of cybercrime on a Bank's finances"., A.R. Raghavan and Latha Parthiban Available at:http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf 10.49 dated 17/03/2020.
14. Lectures on cyber-crime in Delhi H.C. by Adhivakta Parishad on 10/2/2012.
15. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized used or unauthorized access to a computer system.
16. Jargon Dictionary traces the origin of the term 'hacker' to someone who makes furniture with an axe and the term has been used for the first time in 1960's.
17. Ibid

be hacked. Hacking [18] has already become a major problem in India. There have been instances of Indian websites allegedly being hacked by Pakistani hackers. Sometimes back, hackers inserted a link to a pornographic website from the website of SEBI. Hacking is simple to execute and thus the vulnerability of websites is even greater. There are websites, which specialize in hacking and are virtual schools which teach methods of hacking. [19] Many incidences such as first time website of C.B.I. hacked, then Rajasthan Sachivalaya's library and in Jaipur more than 100 sites hacked by hackers.[20] For a simple example anybody who access mobile, without your permission and with bad or malicious intention is a crime. NCRB record said that there is 200% to 300% rise in such crimes and Maharashtra is no.1. Hacking is the nothing but without your permission, deliberately, stealing information like entered computer, now stealing data,[21] stealing programmers, stealing viruses can make new track or road, with this may suffer financial loss. Many times talk time can be steeled by hackers. Once they know password like putting data of Rs. They can put 100Rs.and remaining amount in their account[22]. Illegal access is hacking and for that punishment[23] in IT Act, 2000 [24] as well in IPC1860.[25]

B. Internet Time Theft: - This connotes the usage by unauthorized persons of the internet hours paid for by another person.

C. Data diddling ;- this kind of attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

D. Salami Attack:- Those attacks are used for the commission of financial crimes. The key is here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

18. Webster's Dictionary defines the term hacker as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance.
19. 'Cyber-crime creates demand for network' at http://www.infowar.com.
20. Times of India, 'Yahoo pressed to explain how 500million accounts we hacked. Pune 24/9/2016, pg.18. Col.2-4.
21. Lokmat, "don't give what's up information to Face-Book", Ed. Pune sat. 24/9/2016, pg .9, col. 7-8.
22. News channel, 'sahadri-sakhi', law and security programmed. Guest by Adv. Mali.
23. Sec. 43 (A) gives punishment of imprisonment up to 3 years or with fine which may extend up to 2 lakh or both.
24. Chapter XI Sec. 66 of IT Act, 2000 defines hacking with computer system.
25. In IPC punishment of 3 years or fine of 2 lakh or both and section 420 is applicable.

E. Credit Card Fraud:- This would include cheating, credit card frauds, money laundering etc.[26]

Judicial Response to Cyber Crimes

The issue of cyber-crime in India is primarily dealt with by Information technology Act.(IT ACT) 2000, the Indian Penal Code,(IPC) 1860, The Code of Criminal Procedure, 1973 CR.PC.), The Bankers Book Evidence Act (BBEA) and The Indian Evidence Act (IEA) 1872 etc.[27]

IT has played very important role in the field of banking [28].The IT Act and the amended I P C prescribe various penalties and offences. However it is not only the IT Act that covers cyber-crimes. A large no. of cyber-crimes are actually dealt with by the IPC.[29]The seminar conducted in the presence of Justice Altamas Kabir Judge SC of India, who is also chairman of Cyber Law Enforcement Committee, highlighted the statistics of cyber-crimes cases. There has been little litigation or judicial response to cyber-crimes so far in India and this will be a challenge for judicial decisions on cyber-crime in near future. There has been a landmark judgment on domain dispute in case of ***Rediff Communication Ltd. V. Cyber booth and another***, [30] similarly in ***Yahoo Inc. v. Akash Arora and another*** [31] also the issue of domain name is entitled. Main development has been India's first successful cyber-crime conviction in February. Asif Azim's case matter reported to CBI and he was convicted under section 418,419, and 420 of IPC. The case of ***Yahoo, Inc. v. Akash Arora*** was the first case where an Indian court delivered its judgment relating to domain names. Managing an account segment is the foundation of our economy. The expanding number of digital wrongdoing cases has brought about gigantic loses to our country[32].

Jurisdiction Issues in Internet and Cyber Crime

Jurisdiction is a phase of state sovereignty and it referred to judiciary, administrative and legislative competence. Absence of geographical

26. The Times of India, Friday, Sept. 23, 2016, "caller dupes plumber of $1 L in debit card fraud." Article by Asseem Sheikh.
27. LawZ, Vol.7. No.12 issue 76, Dec.2007. "Cyber Conspiracy or abetment to be treated as Actual Crime.
28. "Online Banking and Cyber Attacks: The Current Scenario", https://www.researchgate.net/publication/290325373 ., 10.32 DATED 17/03/2020.
29. Ibid
30. AIR 200 Bom 27.
31. 1999 PTC (19) 210 (Delhi).
32. "Cyber Crime In Banking Sector"., Harshita Singh Rao * http://oaji.net/articles/2019/1330-1548742941.pdf 10.43 dated: 17/03/2020. 10.40am.

boundaries may give rise to a condition where the material is legal in one country but where it it's posted will violate the laws of that country [33].The main problem of internet jurisdiction is the presence of various parties in the various parts of the world who have an only cyber metric link with each other. So, if one party wants file a suit against other, where he can file? The traditional requirements contain two areas: 1.where the defendant resides; 2.where the cause of action arises. Though these two are difficult to create with any certainty[34]. If the information is power then the right to information is the weapon that helps one to acquire that power[35]. Provisions with respect to internet security jurisdictional aspects. Quicker mode of disport market has tremendous potential for e-commerce with appropriate regulations and infrastructure, India can easily triumph over various global challenges[36]. The world has changed out of all recognition. It took six centuries to move from printed books to T.V. broadcasts. It has taken only six years to move from TV to broadband internet. And this is just the beginning[37]. The 21st century has been labeled as the information age, where civilians are being able to have unprecedented access to information[38]. The world is experiencing the fastened revolution ever after the industrial and green revolution and the revolution is digital revolution[39]. E-banking revolution has fundamentally changed the business of banking by scaling borders and bringing about new opportunities.[40]

Glimpse of Cyber Crimes From the Report of NCRB

A new generation of crime has developed with the advent of computers and internet.[41] Use of modern technology has geared up the business activities. With the emerging trends in business most of the companies are depending on digital money[42]. Karnataka was the first to establish a dedicated police station to handle digital crime 15 years ago. Other states, including UP and Maharashtra, have stepped up police

33. Indian Bar Review, Vol. 46 (1) 2019 p.228.
34. Ibid 228-229.
35. Indian Bar Review, Vol. XXXVI (1 TO 4) 2009. P.148.
36. Indian Bar Review, Vol. XXXIII (1 TO 4) 2006 p.176.
37. Ibid p.161.
38. Indian Bar Review. 45 (1) 2018.
39. Indian Bar Review. 45 (2) 2018.
40."E- Banking , Benfits And Challenges" Mr.Parmanand Barodiya Miss Neema Kumari Jadoun, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/111123/12/first%20paper%20e-banking%20,%20benfits%20and%20challenges.pdf. 10.01am 18/03/2020.
41. Criminal Law Journal, June 2007, "Cyber Crimes in India" By Seyon R. p.135.
42. "Journal of Internet Banking and Commerce Impact Of Cyberattacks On Financial Institutions", Available at: http://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf last Seen on 18/03/2020..11.15am.

training, including seeking out experts from industry[43]. As per PWC's Global Economic Crime Survey, cyber crime has jumped to the second position as the most reported economic crime and financial institutions are prime targets[44] According to research conducted by Indian Computer Emergency Response Team, a total of 27,282 cases have been reported across the world and in India 1 cyber attack is reported ever 10 minutes as against one cyber attack reported in every 12 minutes in the country in the year 2016[45]. ATM frauds, credit cards frauds, biometric frauds, face book wars, What apps war, Fake e-mails or call or SMS, child abuse etc. big challenge today[46]. From 24 hours access to your account, anytime fund transfers and bill payment, but if are not careful, banking from the comfort of your living room opens you up to several security risks[47]. The main threats that a bank faces from cyber attacks include breach of customer data privacy, loss of reputation, business discontinuity, loss of assets/business information, post-breach information etc.[48]

Cyber crime is a fast growing crime in India. The main reason for it is the fact that it is very easy to commit. Bank and online frauds are some of the very serious crimes committed over the cyber world and there are several incident of disseminating unauthorized information, privacy, defamation spreading content over the cyber world where the users are either fully responsible or there is no awareness about the use of the technology underlying it. Such incidents can be reduced by spreading awareness about the technology and about the law[49].

In the past few years, the Indian banking sector has completely transformed[50] The recent financial breach in the Indian banking system

---

43. "How Indian Police is being trained to tackle cybercrime" By Sanghamitra Kar Available at: https://economictimes.indiatimes.com/news/politics-and-nation/karnataka-aims-to-have-one-cyber-crime-post-per-district-by-2019/articleshow/63653447.cms?from=mdr Last seen on 17/03/2020.1.09 pm.
44. "Emerging trends and challenges in cyber security", Nandkumar Saravade, CEO, ReBIT Ambuj Bhalla, Head of SOC, ReBIT Available at: https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security dated 17/03/2020. 11.26 am.
45. Indian Bar Review. 45 (2) 2018.p.151.
46. Indian Bar Review. 45 (2) 2018.p.152-53.
47. "10 Tips for safer online banking". By Lee Munson., Available at: https://nakedsecurity.sophos.com/2013/10/03/8-tips-for-safer-online-banking/ LAST SEEN ON 19/03/2020.12.52pm.
48. "Expert view: Indian banks need to wake up to harsh cyber realities"., Available at: https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms., Last Seen On 19/03/2020. 11.21 am.
49. Indian Bar Review. 45 (3) 2018.p.297..
50. "E-Banking: Challenges And Issues", Available at: https://www.researchgate.net/publication/336950646_E-BANKING_CHALLENGES_AND_ISSUES 9.49am 18/03/2020.

which led to details of over 3.2 million debit cards being compromised, has put a question mark over the security of 'convenient' electronic transactions[51] Banks and various finance companies continuously spread the message to their customers to not pass their bank details passwords to any unknown person over phone, even though a lot of customers come to such trap and send their details. Further bank, insurance companies and their employees pass such personal information to their customers and that information becomes the main reason for such frauds. So, affixing the responsibility on such companies is also very important. Their online transaction process involves outsourcing many copies which in this way lets a lot of people outside these banks get access to personal details of the customers thereby resulting in financial frauds. So a well-defined employee cyber policy along with cyber security policy and awareness is very important to prevent such online fraud incidents across the cyber world[52].

Laws are enacted and various control regimes are providing, but at the end judiciary in any legal system is responsible for the management of justice. In the meantime, cyber-crime is a new event; the judicial reply in the expressions of interpretation of various statutes of cyber law undertakes huge importance. In the case of traditional crimes, there is large number of judicial decisions which perform as a guide, and precedent for easy decisions but it is not so in the case of cyber crimes. It is predictable that in the near future due to the speedy growth and development of technology, administration of justice in cyber-crime and judicial decisions in cyber law will be more challenging[53].

Indian Scenerio

Cyber Crime is a big threat to India'[54]. Online population which loses billions for internet fraud every year, but when it comes to reporting such cases very few seem to come forward. Cyber Crimes are a new class if Crimes rapidly increasing due to extensive use of internet & IT enabled services. India is ranked 5th in the worldwide ranking countries affected by Cyber Crime a report by the Security and Defense Agenda[55].

There are many drawbacks which prevent cybercrimes from being

51. "8 tips to use internet banking safely" By Devansh Sharma Available at: https://economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/articleshow/55113849.cms?from=mdr dated 17/03/2020.12.47pm.
52. Indian Bar Review. 45 (3) 2018.p.228
53. Indian Bar Review , Vol. 46 (2) 2019 p.228
54. Bombay Attacks (2008).
55. "Cyber Crime: A threat to Indian Society, Article on http:// papers.ssrn.com/5013/papers. Abstract _id

solved in India. Conviction in cases of cyber crime in India continues to be abysmally low, even as cybercrime has more than doubled in the last two years, according to the latest home ministry data[56]. Modernization of police force of India is need of the hour. We need Modern police forces that can easily deal with latest technology of electronics and social networking. Where the possibilities of related Crimes and its misuses is to be aware well in advance. [57] .They should take lead in awareness programmer in the general public. Because with growing cases of cyber-crimes in India, people are finding themselves helpless as they are unable to get justice in a timely and proper manner. Government has special reward Package for providing information about hackers.

The irony is that cyber-crime is new age crime and there is no specific law or punishment is penned in Constitution. Most of the defense lawyers are criminal lawyers and their expertise in cyber-crime is limited. The seriousness of offence is most of the cases is quite minor, such as hacking some rivals website, blog or e-mail, money transfer by hacking banks, hacking Government sites and Misusing official website data like heinous crime is rarely traced. Cyber Crime on the rise, but not all cases getting reported by people[58].

Rate of Conviction of those accused of committing cyber-crimes is low but need to fight the threat posed by such offences as it harms the national Security[59]. There are many drawbacks; the law enforcement agencies in the country are not well equipped and knowledgeable enough about cyber-crime. There is immense need for training the law enforcement agencies[60]. Very few cities have cyber-crimes cells. Under the IT Act, the relevant officer entitled to investigate a cyber-crime is a deputy superintendent of police, but most DSP's are not well equipped to fight cyber-crime.[61] There is also lack of dedicated cyber-crime courts in the country where expertise in cyber-crime can be utilized. People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust [62] and without the fear of being harassed. Further, the law enforcement agencies dealing with cyber-

56. "Why most cybercrimes in India don't end in conviction "By Arunabh Saikia, Available at: https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html. Last seen on 27/-3/2020. 1.13pm.
57. Available at: http"//www.gadgeeetsnow.com/technews/governmenttaking steps to curb cyber-crimes in India/.' Tue sept.20, 2016 updated 11.22Am IST.
58. Sneha Shah, "leslie.d@livemint.com posted, on Mon, Dec.19, 2011. 12.53 AM IST.
59. "Government taking steps to curb cyber-crimes in India", on Jul 19, 2016. 2.50 PM. IST.
60. "Computer Crime Research Center (CCRC), Available at: http://www.crime_research.org/news/2003/02/mess/703.htm
61. Ibid
62. Ibid

crime need to come up with an extremely Net savvy and friendly image. In fact it would do India proud if the law enforcement agencies here followed the example set by the Federal Bureau of Investigation in the US and went all out to strengthen the confidence of the people and companies who report cyber-crimes to them.[63]

IT Act 2000 passed in India, is illustrated of the prevailing confusion in the area of jurisdiction[64] in the context of the internet[65]. How India plans to fight the menace of cyber-crime, there is always a big question mark over India. India was considered well equipped and slow when it came to tracking cyber-crime.

IT plays crucial role in personal lives and business.[66] IT solutions today have paved to way to a world internet, business, networking and e-banking budding a solution to reduce cost, change sophisticated economic affair to easier, efficient, speedy time saving methods of transaction. IT was passed in 2000 and amended in 2008, it had many advantages as it gave legal recognition to electronic records, transaction authentications and certification of digital signatures, prevention of computer crimes etc. but it was inflicted with several drawbacks like it does not refer to the protection of IPRS, domain name cyber-squatting so this inhibit the corporate bodies to invest in IT infrastructure, however Cryptography is new phenomenon to secure sensitive information.

Conclusion and Suggestion

Despite the existing corrective and preventive measures undertaken by the government, the attempts at curbing most of these problems have not been successful as evinced by the data mentioned earlier [67] India's central bank, the RBI, has revealed that it discovered around 50,000 cyber frauds in the country's Scheduled Commercial Banks in 2018-19 fiscal[68]To conclude, the Creativity of human mind cannot be checked

63. Ibid

64. Section 1 (2) of IT Act, 2000

65. Narhari v. Pannalal AIR 1977 SC164, Lalji Raja and Sons v. Firm Hansraj Nathuram AIR 1971 SC 974.

66. "An Analysis of Cybercrime Scenario in Pune.", By Mayank R.and Preeti Agarwal, Available at:

https://www.researchgate.net/publication/298801477_An_Analysis_of_Cybercrime_Scenario_in_Pune Last Seen on 17/03/2020. 1.01pm.

67. "Issues Plaguing the Indian Banking Sector" By Sarma D, Kenkre S., Morokole R. Last seen on 18/03/2020. 5.05 pm.

68. "Around 50,000 Cyber Frauds reported in India during 2018-19: RBI", Available at:

https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/ 10.05am 18/03/2020.

by any law, so Prevention, Precaution, Protection, Preservation and Perseverance really holds the key to tackle the problem efficiently. Here are some of the suggestions:

- Absence of international law has complicated the issue because different countries have their National approach to control, regulate and prevent it.
- There must be a Comprehensive International Convention to take Cognizance.
- International Cyber Tribunals need to be constituted to punish the cyber offenders.
- Laws have to be very strict.
- Law enforcement will get. Machinery has to associate with professionals and experts in the field.
- Computer Crime Complaint Centers should be established at district level.
- Lack of expertise
- Computer illiteracy and rampant piracy are factors which contribute to a apathy.
- There must be public education programmer in prevention cyber-crimes.
- Requirement of cyber courts should be a top priority.
- Urgent need for model legislation to tackle the growing influence of Cyber Crime.
- Present IT has several drawbacks the punishment prescribed is only 3yrs. So the country needs to update laws and make punishment harsher.
- The present Law is toothless to determine terrorist groups to combat crimes.
- And finally an eye to eye approach is required to check the Menace.

Online banking is one the most significant developments for the banking industry in its long history. However, despite the many benefits that online banking provides to customers, there are also a number of major concerns and challenges for marketers in the online banking sector[69]

69. "5 Issues and Challenges in The Online Banking Sector", Published by Sheila Mitham ., https://blog.inboundfintech.com/5-issues-and-challenges-in-the-online-banking-sector

References

1. Srivastava Surendra Sahai. Criminology and Criminal Administration. Allahabad: Central Law Agency, 1996.
2. Saxena Manju and Chandra Harish. Law and Changing Society. New Delhi: Deep and Deep Publication Pvt.Ltd. 1999.
3. Dr. Amita Verma. Cyber Crimes and Law, Central Law publications, First Edition: 2009.
4. Indian Bar Review. Vol.XLII (2) 2015.
5. Indian Bar Review. Vol.XLII (2) 2013.
6. An Introduction to Cyber Laws, "By J.P. Mishra, Central Law Publications, 1st Edition. 2012.
7. Information technology, "Law and Practice"., by Vakul Sharma.
8. Dr. J. P. Mishra, "*An Introduction to Cyber Law*"., Central Law Publications .Allahabad., 2nd edition : 2014.
9. Indian Bar Review, Vol. 46 (2) 2019.
10. Indian Bar Review, Vol. 46 (3) 2019.
11. Indian Bar Review, Vol. XXXVIII (3) 2011.
12. Indian Bar Review, Vol. 45 (1) 2018.
13. Indian Bar Review, Vol. XXXIII (1 TO 4) 2006.
14. Indian Bar Review, Vol. XXXVI (1 TO 4) 2009.
15. Indian Bar Review. Vol.XLI (2) 2014.

Webliography

1. "Online Banking and Cyber Attacks: The Current Scenario", https://www.researchgate.net/publication/290325373 .
2. "Cyber-Crime: A Growing Threat To Indian", Seema Goel WEB
3. "Cyber Crime In Banking Sector"., Harshita Singh Rao http://oaji.net/articles/2019/1330-1548742941.pdf
4. "International Research of Journal and Academic Review., "The effect of cybercrime on a Bank's finances"., A.R. Raghavan and Latha Parthiban http://www.ijcrar.com/vol-2-/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf
5. "Cyber Crime in Banking Sector" -Sanchi Agrawal Volume 3, (2016), May "ISSN 2455-2488" http://www.udgamvigyati.org/admin/images/Cyber%20Crime%20in%20Banking%20Sector-%20Sanchi%20Agrawal.PDF
6. "CYBER-CRIMES: A Growing Threat to Indian Banking Sector", By Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru http://www.ijetsr.com/images/short_pdf/1516556483_926-933-SJ99_SIMRAN.pdf

7. "Expert view: Indian banks need to wake up to harsh cyber realities" By Sujan Hajra https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms?from=mdr

8. "A Critical Analysis of Cyber Phishing and its Impact"., by S. Kumudha and Aswathy Rajan https://acadpubl.eu/hub/2018-119-17/2/128.pdf

9. "Journal of Internet Banking and Commerce Impact Of Cyberattacks On Financial Institutions" http://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf

10. "Expert view: Indian banks need to wake up to harsh cyber realities"., https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms.,

11. "Emerging trends and challenges in cyber security", Nandkumar Saravade, CEO, ReBIT Ambuj Bhalla, Head of SOC, ReBIT https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security

12. "8 tips to use internet banking safely" By Devansh Sharma https://economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/articleshow/55113849.cms?from=mdr

13. "8 tips for safer online banking". By Lee Munson., https://nakedsecurity.sophos.com/2013/10/03/8-tips-for-safer-online-banking/

14. What is Internet Banking? What is e-Banking? Available at: https://www.paisabazaar.com/banking/internet-banking-e-banking/

15. "An Analysis of Cybercrime Scenario in Pune.", By Mayank R.and Preeti Agarwal https://www.researchgate.net/publication/298801477_An_Analysis_of_Cybercrime_Scenario_in_Pune

16. "Investigation In Cyber Crime", https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf

17. "How Indian Police is being trained to tackle cybercrime" By Sanghamitra Kar https://economictimes.indiatimes.com/news/politics-and-nation/karnataka-aims-to-have-one-cyber-crime-post-per-district-by-2019/articleshow/63653447.cms?from=mdr

18. "Why most cybercrimes in India don't end in conviction "By Arunabh Saikia https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.

19. "Cybercrime: The Growing Threat To Global Banking" **By Alexander Jones,** *International Banker* https://internationalbanker.com/banking/cybercrime-growing-threat-global-banking/

20. "4 Cyber Attacks that Threaten Financial Inclusion" By Silvia Baur-Yazbeck https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion.

21. TInternet crime: Cyber Crime — A new breed of criminal? By Kit Burden and Creole Palmer https://www.sciencedirect.com/science/article/pii/S0267364903003066

22. "Cyber Crime", https://www.fbi.gov/investigate/cyber

23. 5 Issues and Challenges in The Online Banking Sector

24. Published by Sheila Mitham on August 13, 2017 under online payment https://blog.inboundfintech.com/5-issues-and-challenges-in-the-online-banking-sector

25. "E-Banking:ChallengesAndIssues,"https://www.researchgate.net/publication/336950646_E-BANKING_CHALLENGES_AND_ISSUES

26. "E-Banking: Challenges and Opportunities "Published by: Economic and Political Weekly https://www.jstor.org/stable/4414436?seq=1.

27. "E-Banking In India - Problems And Prospects" By Dr. Lekshmi Bhai.P.S http://troindia.in/journal/ijcesr/vol5iss1part7/77-81.pdf.

28. "E- Banking , Benfits And Challenges" Mr.Parmanand Barodiya Miss Neema, Kumari Jadoun https://shodhganga.inflibnet.ac.in/bitstream/10603/111123/12/first%20paper%20e-banking%20,%20benfits%20and%20challenges.pdf.

29. "Around 50,000 Cyber Frauds reported in India during 2018-19: RBI" https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/

30. http://www.legalserviceindia.com/article+2302682ahtm

31. http://www.thehindu.com/thehindu/mp/2003/01/27/stories/2003012700970100.htm

32. http://shodhganga.inflibnet.ac.in/bitstream/10603/19/19summary.pdf.

33. http://www.rediff.com/business/slide-show/slide-show-1-tech-how-india-plans-to-fight-the-menace-of-cyber.

34. http://papers.ssrn.com/so13/papers.efm?abstract_id-2825079

35. http://www.gadgetsnow.com/tech-news/Government-taking-steps-to-curb-cyber-crimes-in-india/articlesshow/53282039.cms

36. http://articles.economictimes.indiatimes.com/keyword/cybercrime

37. http://www.crime.research.org/news/2003/02/Mess1703.htm.

38. http://hindi.oneindia.com/news/2009/02/01/cybercrime-wef-alok.html

◆ ◆ ◆