JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Regulation Of Artificial Intelligence: Global Perspective

[1]Dr. Nameeta Rana, [2] Manoj Kumar

[1]Assistant Professor, Department of Laws, Himachal Pradesh University Regional Centre, Mohli, Khaniyara, Dharamshala, District- Kangra, H.P.- 176218,

[2]Ph.D. Research Scholar, Department of Laws, Himachal Pradesh University, Summer Hill, Shimla, H.P. -171005

Abstract: Artificial intelligence (AI) can be considered as the biggest innovation with impact comparable to discovery of fire. Artificial intelligence from Turing's time to ChatGPT (model 4) and now Deepseek AI has come a long way. Artificial Intelligence systems are now exhibiting characteristics of intelligence comparable to humans and even exceed it in performing several tasks. Due to this it is becoming more and more difficult to differentiate whether something is real or machine generated. It has various applications as in finance, defence, governance, healthcare, agriculture, education to our personal life which is leading the world to automation in all the sectors. But it has given rise to various crimes due to heavy reliance of this technology on data training and its ability to mimic the tasks so identical to that of humans. Criminals are becoming more difficult to trace and prosecute. Recently, we have seen an increase in new type of crimes such as phishing attacks, digital arrest, cyber fraud, deepfakes and impersonation using audio/video generation tools etc. For all these reasons and many more, the question rises as whether AI should be regulated and how? This article will discuss the recent developments and need for regulation of AI at global scale from Global Data Protection Regulation, Artificial Intelligence Act in Europe to Digital Data Protection Act and proposed Digital India Act in India in light of new digital age challenges keeping in view individual rights, privacy, liability, cyber crimes and cybersecurity.

Keywords: artificial Intelligence, artificial intelligence systems, general purpose artificial intelligence, cybersecurity, data fiduciary, data principal, impersonation, deepfakes, phishing , fake news, chatbots

I Introduction

In the recent years, Artificial intelligence (AI) has become the most sensational innovation with impact as great as the discovery of fire which has shaped the whole human civilization. Artificial Intelligence is new leap in the automation of our world. From the time AI used only in defense to today, it has entered our homes, cars and handheld smart devices and everything has changed as how we interact with cyber space and living world. To go further, firstly we need to understand what Artificial Intelligence is?

Artificial Intelligence (AI) as a term is not a single entity but it is a system of interconnected physical devices such as sensors, optical fibers, displays, computers systems, network transmitter devices, data centers, microchips, underground cables as in computers, smart phones and all connected devices of Internet of things and include intangible things such as programs, codes, data and algorithms.[1] AI deals with the study and making of computer systems with intelligence of some sort comparable to human beings or even greater. These systems are able to learn concepts and tasks that[2] employ modern hardware to do algorithmic calculations [3] and use reasoning and give utility based results about the world, understand human language and even perceive and comprehend visuals.[4] "Artificial Intelligence system" is a machine based system for implicit or explicit goals generates outputs in the form of content, predictions, suggestions and decisions which can influence real or virtual world based on inputs. [5]

In field of AI the objective is to develop such computer systems which are able to perform tasks which require high level of intelligence. AI systems not exactly required to copy human thought process and senses instead in executing some tasks they exhibit such efficiency and effectiveness they may exceed human capabilities.[6] To properly understand AI we need to understand what intelligence means. Some scholars refer to it as rationality which in common parlance means doing "the right thing". [7] Intelligence is the ability of gaining, understanding and applying knowledge rationally and includes all the knowledge gained through senses like visual, sound; imagination; conversation (like reading, writing) and other skills like driving, memorizing, expression and feeling of emotions etc.[8]

Artificial Intelligence is everywhere from defence, healthcare, agriculture, education, business, finance to cars. AI has taken over our personal devices such as smart phones, computers and is becoming integral part of our life with every passing day. We are talking about AI replacing humans at various facilities, workplaces and services. It poses a question whether AI cognition is similar to humans, and if so what about the liabilities. If AI is not completely similar to Human cognition then what is the extent of similarity? If offence is committed by using an AI system how the liabilities will be fixed. Is the owner company of the concerned AI system is responsible or the end user for the illegal use. What about, automated Artificial Intelligence systems as autopilot in cars? If a car in autopilot mode cause an accident how the liability will be fixed. What about the insurance claims. Also, personal data collection by these AI systems poses significant privacy and cyber security risks. Recently we have seen an increase in new type of crimes such as deep fakes, voice mimicking, digital arrests, cyber

[1] Dumouchel, P. (2023). AI and Regulations. *AI*, *4*, 1023–1035. https://doi.org/10.3390/ai4040052

[2] Patternson, D. W. (2023). Introduction to Artificial Intelligence and Expert Systems (13th ed., p. 2) Pearson 2023.

[3] Begishev, I., Asli, M. R., Denisovich, V., Majorov, A., & Sergeyev, A. (2023). Research of artificial intelligence as a subject of crime. *E3S Web of Conferences*, *449*, 03004. https://doi.org/10.1051/e3sconf/202344903004

[4] Patternson, D. W. (2023). Introduction to Artificial Intelligence and Expert Systems (13th ed., p. 2) Pearson 2023.

[5] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 2, C.E.T.S. 225.

[6] Patternson, D. W. (2023). Introduction to Artificial Intelligence and Expert Systems (13th ed., p. 3) Pearson 2023.

[7] Russel, S. & Norvig, P. Intelligence A Modern Approach (4th ed., p.19) Pearson 2023.

[8] Patternson, D. W. (2023). Introduction to Artificial Intelligence and Expert Systems (13th ed., p. 2) Pearson 2023.

frauds, impersonation etc. which are committed using AI technologies. For all these reasons and many more, the question rises as whether AI should be regulated and how?

II. Methodology

This research article discusses the need for regulation of Artificial Intelligence systems in the current digital world across various jurisdictions and making constructive suggestions for the regulation. The methodology used by the researcher is doctrinal in which researcher studied and analysed various statutes, conventions, research paper articles, reports and books to understand and discuss the legislation in respect of use of Artificial Intelligence systems. Keeping the research ethics in view due credit is given to the respective research work cited in this article.

III. Brief History of AI

The term AI is coined by Stanford professor John McCarthy[9] in 1956 who explained it as "the science and engineering of making intelligent machines".[10] In 1950, Alan Turing in his research article "Computing Machinery and Intelligence" created a test presently known as Turing test to differentiate between a task executed by a computer and a human in which a series of questions required to be answered. A computer to pass the test must make the interrogator (human) believe that answers are given by a human and not a machine. According to Turing - computer can perform can perform all the tasks that can be done by human. So, in essence it means that computer cognition is similar to that of a natural person.[11] In the early era of AI research it was assumed that human intelligence is similar to that of an artificial intelligence system and it can be simulated in machines.[12] In 80s Complex systems developed which are equipped with complex reasoning power but they could not self evolve and upgrade their decision making powers, From 90s to 2010 such "Neural networks" developed which are capable of simulating human intelligence in identifying complex patterns and perform complex tasks. Presently using deep learning, neural networks are trained with huge chunks of data and able to mimic human learning patterns and even surpassing human intelligence in many areas.[13] For example-In 2022, ChatGPT came into being which is a generative AI.[14] A China based tech company introduced Deepseek AI [15] surpassing ChatGPT and other AI models in its abilities.

IV. Emerging Threats related to AI

Artificial Intelligence based crimes includes all the illegal acts committed using electronic means such computer, mobiles etc. These crimes are somehow similar traditional crimes as intent to harm can be attributed to them. AI crimes can be

[9] Couch, J. R. (2023). Artificial Intelligence: Past, Present and Future. Journal of South Carolina academy of Science, 21(1), 1. https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1264&context=jscas

[10] Toosi, A., Bottino, A., Saboury, B., Siegel, E., & Rahmim, A (2021, September). A Brief History of AI: How to Prevent Another Winter (A Critical Review). PET Clinics, 16, p. 2. http://dx.doi.org/10.1016/j.cpet.2021.07.001

[11] Turing, A.M.(1950). Computing Machinery and Intelligence. Mind, 59 (236), pp. 433–436. JSTOR. http://www.jstor.org/stable/2251299

[12] Dumouchel, P. AI and Regulations (2023). AI .4(4), 1024. https://doi.org/10.3390/ai4040052

[13] Rigano, C. Using Artificial Intelligence to Address Criminal Justice Needs (2019, January). NIJ journal, 280, 4. https://www.ojp.gov/pdffiles1/nij/252038.pdf

[14] Mohanty, A. & Sahu, S. (2024, November 21) *India's Advance on AI Regulation*. CARNEGIE INDIA. https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india

[15] Ng, k., Drenon, B.,Gerken, T., & Cieslak, M.(2025, February 4*). DeepSeek: The Chinese AI app that has the world talking.* BBC. https://www.bbc.com/news/articles/c5yv5976z9po

committed against individuals, group, State or finance etc.[16] Cyber crimes are generally of two types – firstly, "computer as target crime" in which aim is to destroy or damage computers (tools such as spywares, viruses, Trojans, worms etc. used to attack) and secondly, "computer as tool crime" (computers are used as means to access victims data and commit crimes like cyber fraud, digital arrest, child abuse, digital stalking, deep fakes etc.)[17] Various types of crimes can be committed using AI technology such as integrity attacks, unintended AI outcomes, membership Inference attacks etc. For example- in integrity attacks, false information is entered into a system which compromises the data integrity and produce biased or false results. The risk it projects is creation of "adversarial examples" (a type of integrity attack) i.e. malicious information is injected to manipulate AI systems to produce false results.[18] For example- In 2016, Microsoft launched Tay an AI based chatbot which subjected to integrity attack by the users and gave offensive feedback which is racial, sexiest and abusive. Microsoft has to take it down.[19] It is very difficult to trace such cyber attacks because they can be committed from remote places. Furthermore, new crimes are emerged as explained below:

a. Impersonation (Deepfakes and Voice mimicking)

Modern AI is capable of producing fake content using Generative Adversarial Networks (GANs) which are developed to simulate functions like human brain. With this technology AI can create hyper realistic fake videos and images which are called deepfakes.[20] Some AI models can even mimic the voices of actual people. These advancements have opened a gateway to new crimes using impersonation or identity theft. For example- fake obscene videos are made to blackmail and extort people. Similarly, after impersonating using AI, contact is made to the family members of the individual to extort money.[21] Fake videos of popular public figures are all over the internet. Also, there is spike in spread of fake news and misinformation all over the world.[22] Fake News is posing threats to economy, society, democracy, culture and unity and integrity all over the world. Therefore, digital literacy is important among individuals. People need to be cautious of what they see before believing it and rely only on credible sources for any information.

[16]Qatawneh, I.S.A., Mousa, A.F., Haswa, M., Jaffal, Z., Barafi, J.(2023, January. Artificial Intelligence crimes. Academic Journal of Interdisciplinary Studies, 12(1),144-145. https://doi.org/10.36941/ajis-2023-0012

[17] Jeong, D.(2020, October 7).Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues, IEEE Access, 8, 184562. https://doi.org/10.1109/ACCESS.2020.3029280

[18] Blauth, T.F., Gstrein, O.J., & Zwitter, A. (2022, July 18). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, IEEE Access,10, 77112-77113. https://doi.org/10.1109/ACCESS.2022.3191790

[19] Schesinger, A., O'Hara, K.P., & Taylor, A.S. (2018). Let's Talk About Race: Identify, Chatbots, and AI. CHI 2018. https://doi.org/10.1145/3173574.3173889

[20] Blauth, T.F., Gstrein, O.J., & Zwitter, A. (2022, July 18). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, IEEE Access, 10, 77115. https://doi.org/10.1109/ACCESS.2022.3191790

[21] Chawake, A. (2024, October 30). Beware: How scammers are using AI to sound like your loved ones – 3 tips to stay safe. The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/ai-voice-clone-scams-heres-how-you-can-protect-yourself-9644412/

[22] Caldwell, M., Andrews, J.T.A, Tanay, T. & Griffin, L.D. (2020). AI-Enabled Future Crime, Crime Science, 9(14), 6. https://doi.org/10.1186/s40163-020-00123-8

b. Phishing Attacks

Phishing is a cyber attack in which fake communication in form of digital message is sent to people to access personal information or infect the user system with malware to make user share his personal information such as identity, confidential passwords and bank details. When specific individuals are targeted in such attacks it's called "spear phishing".[23]

c. Fake News

Due to advancement in generative AI fake news content generation is all time high. The fake news content made using AI is so convincing that it shift people's attention from actual information. It is very dangerous as it can shift voting, can cause communal violence and hatred towards specific groups. Fake content is posing threats to economy, society, democracy, culture and unity and integrity all over the world. Therefore, along with stringent law reforms, digital literacy is important among individuals. People need to be cautious of what they see before believing it and rely only on credible sources for any information.[24]

V. Need for Regulation of AI

Artificial Intelligence systems are functioning by collecting data from the users. This poses major risk to privacy and other rights. Hence, calls for stringent data collection and management regulations. Fundamental rights are the basic human rights guaranteed by most of the civil nations to its citizens to ensure their freedom and freewill. As artificial intelligence technologies are being used in governance, monitoring citizens and justice delivery system these rights are under a threat by AI decisions which are not to be discriminated against on ground of religion, race, ethnicity and sex etc. This is due to the fact that law seeks to treat individuals fairly and reasonably but Artificial intelligence technologies develop learning models from the past decisions and give results accordingly. This approach can easily lead to bias decisions and violation of these rights, thus drifting from very essence of law which is justice and fairness.[25] In 2016, United States Supreme Court recognized biasness by Artificial Intelligence tools in fair trial and issued guidelines. The Court made it clear that decisions will cause violation of fundamental rights if made only on basis of prediction of machine learning tools without proper reasoning.[26]

This rapid development of AI technology has caused concerns and challenges for prosecution of AI based crimes. The AI development has given birth to new type of criminals who are capable of using AI algorithms to commit sophisticated cyber-crimes and other illegal activities. Today the legal system is finding itself helpless in detecting and attributing AI based crimes. Criminals are employing AI based tools and anonymity tech to evade prosecution which has made tracing out of attacks and identifying criminals very difficult. Present laws are not clear on liability in such criminal matters and it becomes

[23] Caldwell, M., Andrews, J.T.A, Tanay, T. & Griffin, L.D. (2020). AI-Enabled Future Crime, Crime Science, 9(14), 7-11. https://doi.org/10.1186/s40163-020-00123-8

[24] Caldwell, M., Andrews, J.T.A, Tanay, T. & Griffin, L.D. (2020). AI-Enabled Future Crime, Crime Science, 9(14), 7-11. https://doi.org/10.1186/s40163-020-00123-8

[25] Reed, C.(2018). How should we regulate artificial intelligence?. Royal Society, 376(2128), 2. http://dx.doi.org/10.1098/rsta.2017.0360

[26] *State of Wisconsin v Loomis*, 2016.

more complex to attribute liability in case autonomous AI algorithms are used.[27] Dynamic changes are not made in laws whether they are domestic or international in comparison to rapid development in the media and technology. Present laws seem inadequate in tackling these new types of crimes which are growing in types and numbers with advancement in the technology. Present positive laws across the world are based on the principle of legality that punishment can be given only for breach of law. This principle limits the application of traditional laws in case of emerging cyber crimes.[28] So, AI is like a dual edged sword if used constructively whole world will benefit from it and if misused it can threaten the very existence of humanity. It cannot be denied that malicious use of AI can lead to novel vulnerabilities. Therefore, these threats must be assessed so that proactive measures can be developed to improve cyber resilience.[29]

VI. Regulatory Developments at Global Scale

European Union has passed General Data Protection Regulation (GDPR) which came in force on May 25, 2018. It is a stringent law for protection of privacy and cyber security. Under this law, organizations across the world are made liable as long as they deal with data of people in European Union. GDPR act as a safeguard in cyberspace as it levy hefty fines on violation of its provisions.[30] These regulations act as shield for protection of data and privacy rights when dealing with AI systems.[31]

Europe Framework Convention on AI is a major step taken for use and development of AI technologies ensuring accountability, transparency and fairness.[32] This convention ensures use of AI systems ensuring compliance with human rights, [33]maintaining integrity of democratic processes and rule of law.[34] The convention also binds the party nations to ensure data protection and maintain privacy of individuals[35]; ban discrimination of any sort[36]; muster respect for dignity and individual autonomy[37]; take measures to fix accountability on misuse of AI technology[38] and promote innovation of AI technologies under controlled environment under proper supervision.[39] The convention as per international and domestic

[27] Hifajatali.S,(2024). Artificial Intelligence and Criminal Liability in India: Exploring Legal Implications and Challenges. Cogent Social Sciences, 10 (1),3. https://doi.org/10.1080/23311886.2024.2343195
[28] Qatawneh, I.S.A., Mousa, A.F., Haswa, M., Jaffal, Z., Barafi, J.(2023, January. Artificial Intelligence crimes. Academic Journal of Interdisciplinary Studies, 12(1), 147-148. https://doi.org/10.36941/ajis-2023-0012
[29] Blauth, T.F., Gstrein, O.J., & Zwitter, A. (2022, July 18). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, IEEE Access, 10, 77110-77111. https://doi.org/10.1109/ACCESS.2022.3191790
[30] EU (2018). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/
[31] Chavali,D., Baburajan, B., Gurusamy, A., Dhiman, V.K., Katari,S.C.(2024) Regulating Artificial Intelligence : Developments and Challenges. International Journal of Pharmaceutical Sciences, 2(3), 1255.
[32] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 1, C.E.T.S. 225.
[33] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 4, C.E.T.S. 225.
[34] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 5, C.E.T.S. 225.
[35] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 11, C.E.T.S. 225.
[36] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 10, C.E.T.S. 225.
[37] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 7, C.E.T.S. 225.
[38] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 9, C.E.T.S. 225.
[39] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 13, C.E.T.S. 225.

laws also directs the parties to ensure procedural safeguards[40] and avail remedies to victims by way filing complaint to authorities with jurisdiction in case human rights are violated from activities related to AI system.[41] The convention focus majorly on identifying and assessing risks originating from AI systems. For this purpose, State parties are bound to develop a risk monitoring system, with provision for documentation of risks, testing AI systems before launching them for access and banning them wherever necessary.[42] It is very difficult to tackle potential threats arising from rapid development of AI as regulations alone are not sufficient to stop its misuse. Hence, State parties are required to promote digital literacy and skills among people to keep them safe.[43]

AI Seoul Summit's interim report classifies AI based risks as malicious use risks, risks from malfunctions and systematic risks. Potential risks include- harmful content, cyber security threats, loss of control, privacy violations, discrimination, national security, intellectual property rights violations, global inequality, job displacement by automation etc.[44] For the purpose of policy making, AI related risks can be categorized into malicious risks (creating and distributing harmful AI generated content that could cause human rights violations or threat to public order and safety), algorithmic discrimination (can result in financial losses, loss of opportunity and fundamental rights violations) , transparency failures, systematic risks and loss of control due to lack of human oversight in the development and use of autonomous AI systems, which could result in unintended consequences and threats to national security and public safety.[45]

European Parliament has also taken initiative in regulating development and use of Artificial intelligence by enacting Artificial Intelligence Act. This Act came into force on 1 August, 2024. The Act focuses on safeguarding health, fundamentals rights and safety of people in the European Union while promoting healthy development in the field of Artificial Intelligence. The Act categorizes Artificial Intelligence systems on the ground of associated risks as minimal risk, limited risk, high risk and unacceptable risk. The minimal risk Artificial intelligence systems such as AI based video games and spam filters etc. are not regulated as they pose very low level threat to safety and rights of citizens.[46] Limited risk AI systems are required to aware the user that they are interacting with AI based machine. A few examples are- Content generated by Artificial Intelligence like deepfakes must be marked as such, and users must be aware about emotion recognition AI systems or biometric categorization systems are accessed. The providers of the AI service are required to develop AI system in which AI generated or manipulated content can be identified. Under the Act main priority is given to the regulation of High risk AI systems. Artificial Intelligence systems are considered high risk if they process personal data of individuals such as health, work efficiency, financial situation, interest, behavior or movement etc. High level risk systems

[40] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 15, C.E.T.S. 225.
Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 14, C.E.T.S. 225.
[42] Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 16, C.E.T.S. 225.
Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 20, C.E.T.S. 225.
[44] AI Seoul Summit. (2024). International Scientific Report on the Safety of Advanced AI: Interim Report. https://assets.publishing.service.gov.uk/media/6716673b96def6d27a4c9b24/international_scientific_report_on_the_safety_of_advanced_ai_interim_report.pdf
[45] Mohanty, A. & Sahu,S. (2024). India's Advance on AI Regulation,Carnegie Endowment for International Peace,12. https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india
[46] European Commission, Brussels (2024, August 1). European Artificial Intelligence Act comes into force [Press Release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_4123/IP_24_4123_EN.pdf

are required to develop risk management systems, proper testing and validation of data sets to ensure they are error free. High risk AI systems should ensure proper documentation with inbuilt record keeping in compliance of norms; maintain optimum level of accuracy, human oversight and cybersecurity.[47] AI systems which are dangerous to fundamental rights should be banned. They come under unacceptable risk category. AI applications that can manipulate human behavior and impact free will; "social scoring" systems used by certain States or corporate sector are some of the examples. Certain biometric systems are also banned such emotion recognition systems used to categorize people at workplaces. The AI Act also establishes rules for general-purpose AI models, which are highly competent AI models meant to handle a wide range of activities, such as writing human-like prose. General-purpose AI models are increasingly being employed as components in AI applications. The AI Act would provide transparency throughout the value chain and address any systemic threats from the most proficient models.[48]

VII. Situation in India

India is a growing economy. As a developing nation it is need of the hour to exploit the benefits of artificial intelligence innovations. As artificial intelligence technology has significant potential in boosting economic growth. That's why NITI Aayog has launched "National Strategy for Artificial Intelligence" in June, 2018 to promote research and development in Artificial Intelligence technologies. The intention was to utilize AI technology to boost economic and social development with overall inclusive growth. Mainly five core sectors are identified for this purpose - health, agriculture, education, infrastructure and transportation. The major hurdles in this are shortage of experts in the field of AI, access to intelligent data, higher cost, privacy, security and lack of proper regulations. [49] So, it is apparent that formation of strict regulations is the need of the hour if India seeks to properly integrate AI in economy and governance. From AI perspective, currently the relevant areas of law are cyber laws, privacy laws, intellectual property laws, competition law, media law, employment law, consumer law, criminal law, contract law, and tort law. Major offences related to AI include depiction of a child or an adult in sexually explicit videos which are AI generated, unauthorized impersonation using AI generated deepfakes, discrimination in hiring decisions using AI recruitment tools, use of an individual's personal data without consent to train AI models, misleading ads about reliability or performance of an AI service, use of copyright protected material in AI generated content without permission of the author or owner, catfishing , cyber stalking, cyber bullying and phishing etc. There are certain provisions of statutes which deal with deepfakes in case any AI generated image or video is circulated without consent of the person concerned. There is cheating by impersonation, transmitting obscene material, causing harm to reputation and failure in observing due diligence guidelines for intermediaries.

The rate at which AI is developing it will be difficult to ensure liability under the traditional laws. Digital Personal Data Protection Act, 2023 was enacted to protect the personal data of the individuals and regulate processing of such data for lawful purposes only. The data fiduciaries can only use personal data for which voluntary consent was given by the data

[47] EU (n.d.). High Level Summary of the Artificial Intelligence Act. Retrieved January 8, 2025, from https://artificialintelligenceact.eu/high-level-summary/

[48] European Commission, Brussels (2024, August 1). European Artificial Intelligence Act comes into force [Press Release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_4123/IP_24_4123_EN.pdf

[49] NITI Aayog (2018, June). National Strategy for Artificial Intelligence. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

principal (individual concerned) and nothing else. Data fiduciaries are obligated protect such data, intimate the relevant authorities in case of data breach, erase such data on withdrawal of consent by the concerned data principal. The Act also provides for hefty penalties in case of violation according to gravity. However, there are some concerns over data collection by the instrumentalities of State[50] as it can affect right to privacy. Therefore, Government should draft guidelines for such data collection and processing to mitigate such risk.

Government of India is planning to introduce Digital India Act to replace existing Information Technology Act, 2000 (IT Act, 2000). The present IT Act suffers from various limitations like- lack of exhaustive provisions relating to user rights, online trust and safety; limited ability in recognizing new types of cyber crimes; no specific provisions for dealing with illegal content and regulation of artificial intelligence and machine learning technologies, high risk Automated AI systems and digital businesses; lack of proper adjudication setup and mechanism in case of cybersecurity breach. The proposed Act seeks to create global standard cyber laws to make digital space more secure; create framework for e-governance; promote development in field of AI Technology; create data disclosure norms for intermediaries; address related risks and bestow obligations on digital operators to maintain algorithmic transparency and risk assessment on periodic basis. The Government seeks to ensure fair trade practices in digital space with access to online platforms and digital services without discrimination; safeguard innovation to enable new technologies flourish; regulation of high risk AI systems through algorithmic accountability, vulnerability assessment; and protect rights of digital users such as right to privacy, equality, right to be forgotten, right against discrimination and against autonomous decision making and other constitutional rights and hefty penalties in case of violation.[51] But still, regulations related to Artificial Intelligence in India are in initial stages and have a long way to go as most of these regulations are either in drafting stage or are not currently in force.

VIII. Conclusions and Suggestions

From the above discussion it is clear that Artificial Intelligence is becoming integral part of our life with every passing day. But this fact cannot be ignored that AI systems are feeding on unimaginable amount of data belonging to individuals and organizations. Governments are engaging AI tools in e-governance and justice delivery system. Financial institutions are also employing this technology. Thus, it poses a significant threat to fundamental rights of individuals and also becoming a weapon for crimes. Criminals are exploiting this technology to engage in illegal activities. Therefore, stringent regulations for artificial intelligence systems are must. Also, since AI is gaining human like intelligence with every new version of AI models, related laws cannot be static. Dynamic changes are required to adapt the laws to fix the liabilities if the technology is used for unlawful activities. In this regard Europe has taken vigilant steps by introducing General Data Processing Regulation and now Artificial Intelligence Act with proper data collection, handling, risk based classification of artificial intelligence systems and severe penalties for violations. India though showed intent to make legislative changes to tackle the challenges posed by Artificial Intelligence technology; the regulations are still in the stage of infancy. In today's world data is the new gold and as such it attracts all the good and evil. That's why it must be handled with utmost caution as it not only

[50] Digital Personal Data Protection Act, 2023, §1-17.
[51] Ministry of Electronics and Communication Technology, Government of India (n.d.). Proposed Digital India Act, 2023. Retrieved February 8, 2025, from https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

can impact the rights such as liberty, privacy of the individuals concerned but also control the future of democracies and global peace.

In the end certain suggestions are made in context of building framework for regulation of Artificial Intelligence:

a. Governments should fund research and development of Artificial Intelligence detection tools capable of identifying AI generated content such as deepfakes (audio/ video) like mcAfee deepfake detector[52] to help preventing AI crimes and spread of misinformation.

b. Providers of artificial intelligence systems must be made liable to maintain proper transparency in records of data collected, handled and processed.

c. Users of Artificial Intelligence systems must have right to get their data erased from the servers on demand.

d. Provision for compensation to victims must be there in case user data is mishandled or detrimental use of data.

e. Global treaties should be signed to track and address the AI based crimes as they are normally committed by remote access or through servers situated outside domestic jurisdictions.

f. Regulations alone are not sufficient in tackling Artificial Intelligence based cyber crimes. Digital literacy of the individuals is a must to mitigate the risk of such crimes.[53]

[52] McAfee(n.d.). McAfee Deepfake Detector flags AI-generated audio within seconds. https://www.mcafee.com/ai/deepfake-detector/
[53] Ministry of Electronics and Communication Technology, Government of India (n.d.). Proposed Digital India Act, 2023. Retrieved February 8, 2025, from https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf