INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 4 [2025] | Page 508 - 511

HOW AI IS BECOMING A TOOL FOR INVASION OF PRIVACY

-Shrestha Pal[1]

The very need for artificial intelligence revolves around its ability to continuously gather and analyze raw data, and find solutions for its human user . Through its algorithms, AI meticulously sieves out information , recognizes patterns and manipulates the data to provide the information required by the user . AI models not only use the data to meet human needs and broaden its structure but also to humanize itself.

Without a steady influx of information, AI's growth and progress would be stunted. Therefore, data acts as the life line of artificial intelligence. Given the innate dependence of Artificial Intelligence on data more enhanced algorithms for data collection are being employed.

There are various methods of data collection and these various methods of data collection can also bring more and more problems to the humans.

First off Web scrapping and API integration, it is the process through which large scale data is collected from various websites like social media platforms However it is to be noted that there is a high chance that the data so collected is without the consent of the user it might even go to the extent of violating the terms and conditions of the website and raise ethical and legal concerns.

IOT and data collection, IoT devices and sensors collect data in real time like predictive maintenance and healthcare monitoring , this approach provides real time data ,enhancing data analysis and decision making. The data so collected can also be related to the location of a person or heathcare meaning that the data so collected can often give rise to privacy concerns as there can be surveillance done to collect the data without the explicit consent of the person collecting the data, there can also be potential misuse of the data so collected.

[1] BA. LLB (Hons.) Semester: 7, St. Xaviers University Kolkata

Many data collection models often monitor behavioral patterns of the persons on social media, this can result in intrusive profiling and targeted manipulation. A very evident example of this targeted manipulation can be seen on the analysis of youtube or Instagram feeds of various user as it can be seen that the algorithm shows us media only in accordance to the media which had been previously interacted by the user this also has a social impact as it can result in increased polarization in the society as people do not have an egalitarian world view any more.

The potential for AI to cause harm is not limited to mere unlawful collection or targeted manipulation but especially with the creation of deepfake also extend to identity theft , transmission of fake ai generated intimate images also threatening and blackmailing the victims against the same.

Today's cybercriminals are using generative AI to create hyper-realistic phishing schemes that outpace traditional methods. With just a few clues from social media or public profiles, AI can draft polished, personalized messages or emails that mimic trusted individuals or organizations and can produce thousands of variants in minutes.

These campaigns are highly effective: AI-generated spear-phishing emails achieve click-through rates of around 54%, matching or even exceeding human-crafted attacks (compared to just 12% for generic phishing) Meanwhile, in just a few months AI generated pictures are so realistic that 1 in 4 people struggle to distinguish deepfaked audio—and deepfake videos are fueling a 60% surge in AI-enabled phishing across sectors like finance and healthcare.

These attacks scale sometimes at mere cents per message or they pose a serious threat, bypassing filters and deceiving even trained professionals. In short, AI-powered cybercrime is not just smarter it's faster, cheaper, and eerily convincing, presenting a level of danger that demands equally advanced defenses. Deepfake is created through the collection of data from regards to the victim social media, voice recordings, biometric data , facial images and even data collected from various data breaches. All of this information is collected and the AI system is then trained to replicate the features of the target through various angels, face alignment and swapping is done and further processing is done to manipulate the data to enhance realism. Hence we can see that from the very start the manner in which a deepfake is created that is collection of its raw data goes against the basic tenents of privacy laws.

Now the data so created can be used for identity theft, financial scams etc even if we look at the most technologically advanced countries for example Hongkong's police reports themselves show an estimated loss of 25 million dollars in 2024 by financial frauds committed through the use of AI. So and so there have also been deepfake images of President Joe Biden of USA used to commit election fraud. Moreover deepfake is also used in the creation of sexual images which are then used to further black mail women an example of this is the case of a 19 yr old girl from Charminar who was being black mailed using such pictures, even internationally a student from Indonesia was expelled because of AI generated images.

By now it is well established fact that AI needs data to thrive and survive however AI often weaponizes it and causes data breaches a few ways it can do so include: Cyber attacks caused by AI can be done in various ways it can be through phising schemes or even through the creation of malware designed as spyware or to destroy computers that can generate itself to avoid detection .AI can also be used to detect and use software vulnerabilities.

AI can also help cyber criminals to create APTs that is advanced persistent threats where the intruder gains access to the network for a long period of time and remain un detected for a long period of time. AI can significantly enhance the capabilities of APTs by automating various stages of the attack and continuous adopting of new techniques to remain undetected, These attacks are meticulously planned and executed, often by state-sponsored or highly organized hacking groups, with the intent to steal sensitive data or disrupt operations. Smart, AI-powered ransomware uses machine learning especially natural language processing and reinforcement learning to autonomously scan a system, pinpoint high-value documents, and selectively encrypt only those critical files. This targeted strategy maximizes financial leverage by threatening the most sensitive data, while keeping a low profile by avoiding mass encryption patterns that trigger alerts. By dynamically adjusting encryption speed, algorithm, and timing based on system behavior, such ransomware stays under the radar long enough to complete its attack before detection systems even realize something's amiss

WAY FORWARD

India has made significant strides in data protection with the Digital Personal Data Protection Act (DPDPA), 2023, ensuring user consent and transparency in data usage, yet challenges persist with AI-driven data collection methods like web scraping and IoT devices. The government's investments in AI through initiatives like the IndiaAI Mission aim to foster innovation, but rising AI-powered cyber threats such as deepfakes and phishing demand stronger cybersecurity measures. Ethical AI governance, including bias mitigation and extension in critical sectors, remains a priority, alongside public awareness campaigns to educate citizens on data rights and digital risks. While AI holds immense potential to drive growth in healthcare, agriculture, and governance, balancing innovation with ethical oversight is crucial to ensure equitable and secure technological advancement.