IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Privacy In The Age Of Artificial Intelligence: Challenges And Opportunities

Dr. Jyoti Yadav[1]

Anjali Giri[2]

[1] Prof at Amity Law University , Amity University Lucknow Uttar Pradesh 226010
[1] Scholar at Amity Law University , Amity University Lucknow Uttar Pradesh 226010

Abstract

In an increasingly interconnected world, the ability of artificial intelligence (AI) to process analyze, and infer patterns from data introduces risks of unintended data exposure, discrimination, and misuse of personal information. As AI technologies advance, they present fundamental privacy challenges alongside transformative opportunities. AI systems, powered by vast amounts of data, have the potential to revolutionize industries, improve services, and enhance user experiences. However, this progress raises serious concerns about the erosion of personal privacy, surveillance, and the security of sensitive information. This study examines the intricate relationship between privacy and AI, along with the ways existing privacy frameworks are being modified and tested to address these new challenges. The ethical ramifications of AI systems and the role of regulation in defending individual rights are also assessed. The study suggests methods for achieving a balance between privacy protection and innovation, including enforcing stricter data governance regulations, promoting privacy- preserving technologies like federated learning and differential privacy, and ensuring transparency in AI decision-making. Ultimately, cooperation between technology developers, regulators, and society will determine the future of privacy in the AI era, ensuring that advancements in AI align with the protection of individual privacy and fundamental human rights.

[1] Prof at Amity Law University , Amity University Lucknow Uttar Pradesh 226010
[2] Scholar at Amity Law University , Amity University Lucknow Uttar Pradesh 226010

I. Introduction

The right to privacy is a fundamental aspect of many legal systems that aim to limit both government and private actions that may infringe upon individual privacy. More than 185 national constitutions recognize this right. Following the global surveillance revelations in 2013, privacy has become a focal point of international discourse. Agencies such as the NSA, FBI, CIA, RAW, and GCHQ have engaged in extensive global surveillance activities. Current

discussions regarding privacy revolve around several key issues: the compatibility of privacy with the capabilities of intelligence agencies to access and scrutinize personal information, whether individuals relinquish their right to privacy as part of a social contract to enhance security against perceived terrorist threats, and whether the justification of terrorism constitutes a legitimate rationale for monitoring the general populace. Additionally, private sector entities, particularly technology firms like Amazon, Apple, Meta, Google, Microsoft, and Yahoo, pose significant risks to privacy by collecting and utilizing personal data.

II. Right to Privacy

Respect for privacy is regarded as a fundamental right of individuals in many international treaties. It is essential for maintaining human dignity and is one of the core components of a democracy. It upholds both individual rights and those of others. The concept of privacy is not new, ancient Greece recognized divisions between Polis and Oikos, referring to the public or political realm and the private or familial sphere, respectively. However, the "right" to privacy is a relatively contemporary notion.

The concepts of privacy and the right to privacy can be challenging to understand. Privacy often pertains to modern information and communication technologies and is grounded in the principle of natural rights. The right to privacy encompasses our ability to protect our personal spaces, including our bodies, homes, assets, ideas, feelings, secrets, and identities.

The Supreme Court has chosen to interpret Article 21 in conjunction with the Universal Declaration of Human Rights to broaden its application. The Constitution of India does not explicitly endorse the right to privacy as a fundamental libertarian ideal. In Kharak Singh v. State of U.P.[3], the issue of surveillance of suspects highlighted the emergence of the right to privacy.

[3] 1962

III. History of Right to Privacy

The concept of a human "right to privacy" begins when the Latin word ius expanded from meaning "what is fair" to include "a right – an entitlement a person possesses to control or claim something," by the Decretum Gratiani in Bologna, Italy in the 12th century.

In the United States, an article in the 15 December 1890, issue of the Harvard Law Review entitled "The Right to Privacy," written by attorney Samuel D. Warren II and future U.S. Supreme Court Justice Louis Brandeis, is often cited as the first explicit finding of a U.S. right to privacy. Warren II and Brandeis wrote that privacy is the "right to be let alone," and focused on protecting individuals. This approach was a response to recent technological developments of the time, such as photography and sensationalist journalism, also known as "yellow journalism."

Privacy rights are inherently intertwined with information technology. In his widely cited dissenting opinion in Olmstead v. United States[4], Brandeis relied on thoughts he developed in the article "The Right to Privacy." In that dissent, he urged that personal privacy matters were more relevant to constitutional law, going so far as to say that "the government was identified as a potential privacy invader." He writes, "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." At that time, telephones were often community assets, with shared party lines and potentially eavesdropping switchboard operators. By the time of Katz, in 1967, telephones had become personal devices with lines not shared across homes and switching was electro-mechanical. In the 1970s, new computing and recording technologies raised more concerns about privacy, resulting in the Fair Information Practice Principles. In recent years, there have been few attempts to clearly and precisely define the "right to privacy.

[4] 1928

[5] 1962

IV. Right to Privacy in India

The Right to Privacy is one of these rights since the right to life in Article 21 is flexibly defined to cover all parts of a person's existence that make their life more meaningful. The Supreme Court ruled that Regulation 236 of the UP Police Regulations breached the Constitution because it violated Article 21 of the Indian Constitution in Kharak Singh v. the State of UP[5], which was the first case to address this issue of the right to privacy.

The Court ruled that the right to privacy is intertwined with the right to preserve individual life and personal liberty. In its ruling, the court linked individual freedom with privacy.

In Maneka Gandhi v. UOI (1978), the court established the triple test for any law restricting individual freedom such as: It must outline a process,
The approach must pass the test of one or more Article 19-granted fundamental rights that might be applicable in a particular circumstance. It must pass Article 14 scrutiny.

Right to Privacy Article 21

The Article 21 of the Indian Constitution mentions the Right to life and the Right to personal liberty. Everyone has the right to life and the right to personal liberty, both citizens and noncitizens, according to this article. These two rights cannot be taken away from anyone by the state unless certain conditions are met, as outlined by the Indian Penal Code. Under the K.S. Puttaswamy case[3], SC held that the right to privacy was also included in the right to life and liberty.

V. What is AI?

Artificial Intelligence (AI) refers to the development of computer systems of performing tasks that require human intelligence. AI aids, in processing amounts of data identifying patterns and making decisions based on the collected information. This can be achieved through techniques like Machine Learning, Natural Language Processing, Computer Vision and Robotics. AI encompasses a range of abilities including learning, reasoning, perception, problem solving, data analysis and language comprehension. The ultimate goal of AI is to create machines that can emulate capabilities and carry out diverse tasks, with enhanced efficiency and precision.
The field of AI holds potential to revolutionize aspects of our daily lives.

Artificial Intelligence (AI) has become increasingly integrated into various aspects of our lives, revolutionizing industries and impacting daily routines. Here are some examples illustrating the diverse applications of AI:

[3] Justice KS Puttasamy vs Union Of India & Ors. 2017 , commonly known as Right to Privacy Verdict

5.1 Virtual Personal Assistants: Popular examples like Siri, Google Assistant, and Amazon Alexa utilize AI to understand and respond to user commands. These assistants employ natural language processing (NLP) and machine learning algorithms to improve their accuracy and provide more personalized responses over time.

5.2 Autonomous Vehicles: AI powers the development of self-driving cars, trucks, and drones. Companies like Tesla, Waymo, and Uber are at the forefront of this technology, using AI algorithms to analyze sensory data from cameras, radar, and lidar to make real- time driving decisions.

5.3 Healthcare Diagnosis and Treatment: AI algorithms are used to analyze medical data, including patient records, imaging scans, and genetic information, to assist healthcare professionals in diagnosing diseases and planning treatments. IBM's Watson for Health and Google's DeepMind are examples of AI platforms employed in healthcare.

5.4 Recommendation Systems: Online platforms like Netflix, Amazon, and Spotify utilize AI to analyze user behaviour and preferences, providing personalized recommendations for movies, products, and music. These systems employ collaborative filtering and content-based filtering techniques to enhance user experience and increase engagement.

5.5 Fraud Detection: AI algorithms are employed by financial institutions to detect fraudulent activities in real-time. These systems analyze.

VI. Types of AI

There are different types of AI, often categorized into:

6.1 Narrow AI (Weak AI): This type of AI is designed to perform a specific task, such as voice recognition (like Siri or Alexa), recommendation systems (like Netflix suggestions), or image recognition. It's very good at what it does, but it doesn't possess general intelligence or consciousness.

6.2 General AI (Strong AI): This would be a form of AI capable of performing any intellectual task that a human can do, with the ability to understand, learn, and apply knowledge across a wide range of tasks. It remains largely theoretical at this point.

6.3 Superintelligent AI: A hypothetical future AI that surpasses human intelligence in every possible aspect. It would be able to outperform humans in all cognitive tasks, including creativity, social intelligence, and problem-solving. This level of AI is still speculative and presents both exciting opportunities and significant ethical challenges.

VII. How Does AI Work?

Artificial Intelligence (AI) uses a wide range of techniques and approaches that enable machines to simulate human-like intelligence and perform tasks that traditionally require human assistance. AI systems work through a combination of algorithms, data, and computational power. Here's an overview of how AI works:

7.1 Data Collection: AI systems rely on vast amounts of data to learn and make decisions. Data can be collected from various sources, including sensors, digital devices, databases, the internet, and user interactions. The quality and quantity of data are crucial for training accurate and reliable AI models.

7.2 Data Pre-processing: Once data is collected, it needs to be pre-processed to ensure it's clean, structured, and suitable for analysis. This pre-processing stage may involve tasks such as cleaning noisy data, handling missing values, standardizing formats, and encoding categorical variables.

Algorithm Selection: AI algorithms are chosen based on the specific task or problem the AI system aims to solve. Different algorithms are suited for different types of tasks, such as classification, regression, clustering, and pattern recognition. Common AI algorithms include neural networks, decision trees, support vector machines, and k- nearest neighbours.

7.3 Model Training: In the training phase, AI models are fed with labelled data (supervised learning) or unlabelled data (unsupervised learning) to learn patterns and relationships. During training, the model adjusts its parameters iteratively to minimize errors and improve its performance on the given task. This process involves optimization techniques like gradient descent and backpropagation in neural networks.

7.4 Model Evaluation: After training, the AI model is evaluated using separate validation data to assess its performance and generalization ability. Performance metrics such as accuracy, precision, recall, F1-score, and area under the curve (AUC) are used to quantify the model's effectiveness in making predictions or decisions.

7.5 Model Deployment: Once the AI model meets the desired performance criteria, it can be deployed into production environments to perform real-world tasks. Deployment involves integrating the model into existing systems, such as mobile apps, web services, or embedded devices, to provide AI-driven functionalities.

7.6 Continuous Learning and Improvement: AI systems can adapt and improve over time through continuous learning. They can be updated with new data and retrained periodically to stay relevant and accurate in dynamic environments. Techniques like online learning, transfer learning, and reinforcement learning enable AI models to learn from new experiences and feedback.

7.7 Inference and Decision-Making: During inference, the trained AI model applies its learned knowledge to make predictions or decisions on new, unseen data. Inference involves feeding input data into the model and obtaining output predictions or classifications based on the model's learned patterns and representations.

VIII. Reflection of AI on Privacy

The rise of Artificial Intelligence (AI) has a profound impact on privacy, both positively and negatively. Here's how AI intersects with privacy:

Positive Impacts:

8.1 Enhanced Privacy Protection Tools: AI can help improve privacy protection by developing smarter encryption methods, anomaly detection systems, and cybersecurity measures that can detect and prevent unauthorized access or data breaches more effectively than traditional methods.

8.2 Personalized Privacy Settings: AI can enable individuals to have better control over their privacy by creating tools that automatically adjust privacy settings based on user preferences and behaviorS . For example, AI could help you fine-tune your data-sharing settings across various online platforms, ensuring that only the data you wish to share is shared.

8.3 Improved Data Masking and Anonymization: AI can also help anonymize sensitive data, ensuring that personal identifiers are removed or masked before sharing the data. For instance, AI can be used in medical research to create datasets that preserve privacy by de- identifying patient information.

Negative Impacts:

8.4 Data Collection and Surveillance: AI systems often require vast amounts of data to function effectively. This can lead to the collection of massive amounts of personal information, raising concerns about surveillance and data privacy. For instance, AI powered systems like facial recognition and tracking technologies can be used to monitor individuals in public spaces without their consent, infringing on personal privacy.

8.5 Invasive Data Usage: AI can be used to mine and analyze personal data from various sources (social media, browsing habits, purchase history) to create highly detailed profiles of individuals. While this data may be used for personalized ads or services, it can also be exploited for purposes that the individual never agreed to, leading to privacy violations.

8.6 Lack of Transparency and Control: Many AI systems operate as "black boxes," meaning users don't fully understand how their data is being used or how decisions are made. This lack of transparency can lead to privacy concerns, as individuals may not know how their personal information is being accessed or shared. In some cases, AI systems may even make decisions that affect people's lives (e.g., credit scoring or hiring processes) based on personal data without giving users the ability to challenge or control how that data is used.

8.7 Bias and Discrimination: AI systems are trained on data, and if that data contains biases, the AI can perpetuate or even amplify those biases. This can have privacy implications, particularly when sensitive data (such as race, gender, or socioeconomic status) is used. If not carefully managed, AI can lead to discriminatory practices that violate an individual's right to privacy and fair treatment.

8.8 Data Breaches: AI systems can sometimes be vulnerable to hacking or malicious attacks. When AI tools store or process large amounts of personal data, these systems become attractive targets for

cybercriminals. A breach could expose sensitive personal information, leading to significant privacy risks.

IX. Cyber Attacks affecting Privacy

Cybercrimes that affect privacy involve illegal activities that compromise an individual's or organization's personal information, data, or online security. These crimes are often carried out by cybercriminals who exploit technological vulnerabilities or engage in malicious activities to access, steal, or misuse personal data. Here are some of the most common cybercrimes affecting privacy:

9.1 Identity Theft • Description: Cybercriminals steal personal information (such as Social Security numbers, credit card details, or login credentials) and use it to impersonate the victim for fraudulent purposes. This may involve opening bank accounts, making unauthorized purchases, or committing other types of financial fraud. • Impact on Privacy: Identity theft can severely compromise privacy, as the criminal has access to a person's personal, financial, and sometimes professional details. Victims may face long-term consequences, including damaged credit scores and financial loss.

9.2 Phishing • Description: Phishing involves cybercriminals using deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or other personal details. Often, these phishing attempts appear to come from trusted sources (e.g., banks, government agencies, or popular services). • Impact on Privacy: Phishing attacks can lead to the unauthorized disclosure of private data, allowing criminals to access accounts, steal money, or carry out other malicious actions, compromising an individual's privacy.

9.3 Data Breaches • Description: A data breach occurs when unauthorized individuals access a database or system to steal sensitive data. These breaches can target businesses, healthcare institutions, government agencies, or any organization that stores personal information. Hackers may access millions of records, including emails, passwords, addresses, financial data, and health information. • Impact on Privacy: Data breaches expose personal information to the public or black market buyers, putting individuals at risk of identity theft, fraud, and other privacy violations. In some cases, sensitive data such as medical records or social security numbers can be exploited.

9.4 Ransomware Attacks • Description: Ransomware is malicious software that encrypts a victim's data, rendering it inaccessible, and demands a ransom for its release. Often, ransomware attacks target large organizations but can also affect individuals who store personal data on their devices. • Impact on Privacy: In addition to the financial impact of paying the ransom, victims may suffer from the exposure of personal data if the attackers threaten to leak or sell the stolen information. Privacy is directly compromised as criminals gain access to sensitive information and files.

9.5 Spyware and Malware • Description: Spyware is a type of malicious software designed to secretly monitor a user's activities, capture personal information (such as login credentials, credit card numbers, or browsing habits), and send it to cybercriminals without the victim's consent. It can be installed on a victim's device through infected downloads, phishing emails, or other malicious

software. • Impact on Privacy: Spyware invades privacy by continuously collecting data from the victim's device, including sensitive personal details, internet activity, and even conversations. It can lead to identity theft, financial loss, and the leakage of personal or confidential information.

9.6 Social Engineering Attacks • Description: Social engineering is the art of manipulating individuals into divulging confidential or personal information by exploiting human psychology. Examples include pretexting (posing as a trusted figure), baiting (offering something in exchange for information), or tailgating (gaining physical access to a secure area). • Impact on Privacy: Social engineering attacks exploit a victim's trust, leading them to reveal sensitive information that can be used to violate their privacy, steal identities, or access confidential accounts.

9.7 Man-in-the-Middle Attacks • Description: In a man-in-the-middle (MITM) attack, cybercriminals intercept communications between two parties (such as between a user and a website) to steal sensitive information. This type of attack can occur on unsecured networks, such as public Wi-Fi. • Impact on Privacy: MITM attacks expose private communications, login credentials, credit card numbers, and other personal data to criminals who can misuse this information for malicious purposes.

9.8 Stalking and Harassment (Cyberstalking) • Description: Cyberstalking involves the use of digital tools (such as social media, email, or other online platforms) to stalk, harass, or intimidate an individual. The perpetrator may track the victim's movements, read private messages, or even threaten them with public exposure. • Impact on Privacy: Victims lose control over their personal space and online presence. Their privacy is violated as cyberstalkers monitor their every move online, sometimes using private information to harass or threaten them.

9.9 Doxxing • Description: Doxxing involves publicly releasing or publishing private information such as home addresses, phone numbers, or personal history) without the victim's consent, [9] usually with malicious intent. It is commonly done through social media platforms or public forums. • Impact on Privacy: Doxxing exposes personal information to the public, often leading to harassment, threats, or even physical harm. It violates the victim's right to privacy by making personal information accessible to anyone online.

9.10 Insider Threats • Description: An insider threat occurs when an employee or trusted individual within an organization intentionally or unintentionally accesses sensitive information and exposes it to unauthorized individuals. This could involve stealing customer data or disclosing confidential internal documents. • Impact on Privacy: Insider threats can compromise sensitive business information and personal data, leading to privacy violations, reputational damage, or even financial losses for individuals or organizations.

9.11 Cryptojacking • Description: Cryptojacking is when cybercriminals secretly use a victim's computer, smartphone, or other devices to mine cryptocurrency without the owner's consent. This is usually done by infecting a device with malware. • Impact on Privacy: While cryptojacking itself doesn't directly involve stealing personal data, it can give attackers unauthorized access to a victim's

device. This could potentially be used as a launching point for further privacy violations, such as spying on the victim's activities.

9.12 Fake Wi-Fi Networks (Evil Twin Attacks) • Description: In an "evil twin" attack, cybercriminals create a fake Wi-Fi network that looks like a legitimate public network (e.g., in a café or airport). When users connect, their data is intercepted by the attacker. • Impact on Privacy: If a user connects to a fake network, cybercriminals can intercept private communications, such as login credentials, emails, and financial transactions, violating the user's privacy and stealing sensitive information.

X. Right to Privacy SC Judgements

Although Article 21 does not mention the right to privacy directly, the Supreme Court of India has expanded the scope of Article 21 in a number of cases. There are other such SC decisions, the most significant are listed below.

i. AK Gopalan vs the State of UP 1950 In this case, the petitioner argued that the police search and seizure on his property violated his right to property under Article 19 of the Constitution.

However, the court dismissed his privacy claim, saying the police action didn't stop him from using his property. The court also pointed out that police have the right to search and seize if they have 'reasonable cause.'

ii. Kharak Singh vs the State of UP 1963 In this case, the petitioner said that the police's latenight visits to his home violated his right to travel freely under Article 19 of the Indian Constitution. He also complained about the police following him. The court agreed that the late-night visits violated his right to live freely and with dignity. However, it ruled that the right to privacy is not a fundamental right, so monitoring his activities was not against the law.

iii. Justice K.S. Puttaswamy vs Union of India 2017 The Supreme Court of India unanimously decided during the hearing of a suit that questioned the constitutional legality of the Aadharbased biometric system that the right to privacy is a fundamental right protected by the Constitution.

The court widened the scope of Article 21 and declared that the right to privacy is also included in the right to life and liberty as guaranteed by that provision. The right to privacy so immediately became a fundamental right following the judgement because Article 21 is covered by Part III of the Indian Constitution, which addresses fundamental rights. Since that time, India has seen the right to privacy as a Fundamental Right of the person.

XI. Right to Privacy Supreme Court's Aadhar Judgement

Residents have the right to obtain an Aadhaar number under the Aadhaar Act by enrolling and providing biometric and demographic data. The Aadhaar Act's provisions were scrutinised by the Supreme Court to see if they violated the right to privacy, which the Supreme Court recognised as a fundamental right in 2017. It's important to note that many services offered by both the government and commercial companies

needed users to link their Aadhaar numbers for authentication, effectively making getting an Aadhaar number necessary for the great majority of people.

Because of this, the real dispute was whether this was a legal exception rather than whether it violated someone's right to privacy. Due to their failure to adhere to the aforementioned proportionality requirement, the Supreme Court invalidated or reduced some provisions of the Aadhaar Act. Aside from these clauses, the Supreme Court determined that the Aadhaar Act functions as a reasonable exemption to the right to privacy since it is appropriate and serves a legitimate state aim.

XII. Right to Privacy Related Government Initiatives

The government has taken steps by enacting laws for the protection of privacy of the Indian citizens which are discussed below:

i. Information Technology Act of 2000

The Information Technology Act of 2000 is a law in India that governs electronic commerce, digital signatures, and the protection of sensitive information such as personal data. The act was enacted with the goal of regulating the use of electronic communication and digital signatures and providing legal recognition to transactions carried out through electronic means.

It offers a defence against some computer system data breaches. It has security measures to stop unauthorised access to computers, computer systems, and the data kept on them.

ii. Personal Data Protection Bill 2019

To establish a Data Protection Authority of India for these purposes and matters relating to an individual's personal data, as well as to provide for the protection of individuals' privacy in connection to their personal data. Considering the suggestions made by the B N Srikrishna Committee (2018).

XIII. Limitations on the Right to Privacy in India

In India, many laws protect the right to privacy, but there are some limitations. The Indian Penal Code, of 1860 allows for restrictions on this right to ensure national security, public order, and morality, or in cases like judicial contempt and defamation.

The Supreme Court has stated that the right to privacy is not absolute and can be limited for public welfare and national security. It may also be restricted to prevent crimes.

Also, the government can conduct surveillance, intercept communications, or collect biometric data, especially in matters involving foreign individuals or groups important for national security.

Individuals may also choose to waive their right to privacy when they share personal information with companies for services or contracts.

i. Shreya Singhal v. UOI

In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court.

Facts: Two women were arrested under Section 66A of the IT Act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishmentif any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will.The women, in response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and

expression.

Decision: The Supreme Court based its decision on three concepts namely: discussion, advocacy, and incitement. It observed that mere discussion or even advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was found that Section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder, security, health, and so on.

ii. Shamsher Singh Verma v. State of Haryana

In this case, the accused preferred an appeal before the Supreme Court after the High Court rejected the application of the accused to exhibit the Compact Disc filed in defence and to get it proved from the Forensic Science Laboratory.

iii. Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr.

Facts: The subscriber purchased a Reliance handset and Reliance mobile services together

under the Dhirubhai Ambani Pioneer Scheme. The subscriber was attracted by better tariff plans of other service providers and hence, wanted to shift to other service providers. The petitioners (staff members of TATA Indicom) hacked the Electronic Serial Number (hereinafter referred to as "ESN"). The Mobile Identification Number (MIN) of Reliance handsets were irreversibly integrated with ESN, the reprogramming of ESN made the device would be validated by Petitioner's service provider and not by Reliance Infocomm. Questions before the Court: i) Whether a telephone handset is a "Computer" under Section 2(1)(i) of the IT Act?

1. ii) Whether manipulation of ESN programmed into a mobile handset amounts to an alteration of source code under Section 65 of the IT Act?

Decision: (i) Section 2(1)(i) of the IT Act provides that a "computer" means any electronic, magnetic, optical, or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Hence, a telephone handset is covered under the ambit of "computer" as defined under Section 2(1)(i) of the IT Act.

(ii) Alteration of ESN makes exclusively used handsets usable by other service providers like TATA Indicomm. Therefore, alteration of ESN is an offence under Section 65 of the IT Act because every service provider has to maintain its own SID code and give its customers a specific number to each instrument used to avail the services provided. Therefore, the offence registered against the petitioners cannot be quashed with regard to Section 65 of the IT Act.

iv. Shankar v. State Rep.

Facts: The petitioner approached the Court under Section 482, CrPC to quash the charge sheet filed against him. The petitioner secured unauthorized access to the protected system of the Legal Advisor of Directorate of Vigilance and Anti-Corruption (DVAC) and was charged under Sections 66, 70, and 72 of the IT Act.

Decision: The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act.

XIV. Conclusion

As we navigate the intricate landscape of AI's swift advancement, the challenge of privacy stands out as one of the most pressing issues of our era. While AI presents significant opportunities for innovation, efficiency, and tailored experiences, it simultaneously introduces critical ethical and security dilemmas concerning the collection, utilization, and safeguarding of personal information. The capacity of AI systems to process and analyze extensive data has revolutionized business operations and government-citizen interactions, yet it has also heightened the risks of surveillance, data misuse, and inadvertent biases.

To ensure that AI benefits society in a responsible and equitable manner, it is crucial for privacy protections to advance in tandem with technological progress. This necessitates a cooperative approach among developers, policymakers, and the public to create comprehensive data governance frameworks that emphasize transparency, consent, and accountability.

Furthermore, as AI technologies continue to develop, the ethical standards guiding their design and application must also evolve, ensuring that privacy is integrated into their foundational principles rather than considered a secondary concern.

In conclusion, protecting privacy in the age of AI will require continuous effort, striking a balance between fostering innovation and upholding the essential right to personal privacy. By cultivating a culture of responsibility, awareness, and accountability, we can ensure that the potential of AI is realized in ways that honor individual rights and contribute to a more just and secure digital landscape.

XV. Acknowledgement

I would like to express my gratitude to the following organizations and individuals for their invaluable support in completing this research project.
First of all, I would like to express my sincere gratitude to Dr Jyoti Yadav for his/her support and guidance throughout the doctoral programme. Dr Jyoti Yadav’s insights and feedback have been helpful in shaping the scope and directions of this study.
I am also grateful to my colleagues for their assistance with data collection, analysis, and interpretation, which made the study possible.
I would also like to express my gratitude to the members of research committee for their constructive criticism and valuable feedback, which contributed to enhancing the quality of this research.
Finally, I thank Amity Law School, Amity University for providing the necessary facilities and resources to conduct my research.
I extend my gratitude to all for your invaluable contributions that significantly enhanced the quality of the paper.

Refferences

1. Indian Constitutionhttps://legislative.gov.in/constitution-of-india
2. Right to Privacy Article 21https://indiankanoon.org/
3. SC judgements https://indiankanoon.org/