RIGHT TO PRIVACY IN THE ERA OF INTERNET

Shruti Khelwari, B.A. LL.B., KES's Shri Jayantilal H Patel College of Law

Shreya Khewalri, B.A. LL.B., KES's Shri Jayantilal H Patel College of Law

ABSTRACT

In the digital age in the context of modern technology and the internet. It examines the legal frameworks that govern, the right to privacy has become a critical concern, particularly with the rapid expansion of the internet. This paper explores the evolution and challenges of privacy rights privacy, including international conventions, national laws, and judicial interpretations. The paper also addresses the complex issues arising from data collection, surveillance, and the dissemination of personal information by both state and private entities. A key focus is the balance between ensuring individual privacy and the need for security, as well as the role of social media platforms, data-driven companies, and government agencies in shaping privacy standards. Additionally, the paper analyzes recent legal developments, Data protection policies and statistics, and the implications of these laws on global privacy practices. By exploring the tension between privacy rights and technological advancements, the study aims to highlight the importance of protecting individual freedoms while ensuring a safe and secure online environment. The paper concludes by proposing potential legal reforms and ethical guidelines to safeguard privacy in the digital era.

INTRODUCTION

The digital revolution has fundamentally altered the way individuals interact, work, and navigate the world. With the widespread availability of the internet, personal data is constantly being generated, shared, and analyzed, raising pressing concerns about privacy in an era of rapid technological advancement. From social media interactions and e-commerce transactions to smart devices and artificial intelligence, nearly every aspect of life today leaves behind a digital footprint. While this has undoubtedly enhanced efficiency and convenience, it has also given rise to significant debates about the boundaries of privacy, the extent of surveillance, and the potential risks associated with data collection.

As researchers and policymakers examine these concerns, it becomes evident that privacy in the digital space is a complex issue with multiple dimensions. On one hand, digital platforms rely on user data to personalize experiences, improve services, and drive economic growth. On the other hand, the increasing dependence on data-driven technologies has made individuals more vulnerable to breaches, unauthorized access, and misuse of personal information. Studies suggest that while users often consent to data collection through terms of service agreements, the extent to which they fully understand these agreements remains questionable. This raises ethical questions about informed consent and the power dynamics between users, corporations, and governing bodies in the digital landscape.

The legal recognition of privacy as a fundamental right has been an evolving process, with many jurisdictions attempting to establish safeguards against intrusive data practices. In some regions, regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) have set stringent guidelines on data protection, emphasizing transparency and user control. In contrast, other parts of the world still grapple with outdated or fragmented privacy laws that struggle to keep pace with the rapid evolution of digital technologies. The ongoing discourse around digital privacy often highlights the tension between economic interests, national security, and individual rights, making it a challenging issue to regulate effectively.

despite legal advancements, concerns persist regarding the effectiveness of enforcement mechanisms, the reach of state surveillance, and the obligations of corporations handling vast amounts of user data. The interplay between technological development and regulatory oversight continues to shape the evolving discourse on digital privacy in the country.

Additionally, the risks associated with cybersecurity breaches have further intensified discussions on digital privacy. As organizations and institutions collect and store massive datasets, the threat of cyberattacks, identity theft, and financial fraud has become a growing concern. Reports suggest that inadequate security measures, coupled with a lack of awareness among users, have contributed to an environment where personal information is often exposed to exploitation. The rise of artificial intelligence and machine learning further complicates the landscape, as predictive algorithms analyze vast amounts of data, sometimes leading to unintended biases or ethical dilemmas regarding data use.

Given these complexities, discussions on digital privacy continue to evolve, with multiple perspectives shaping the way forward. Some advocate for stronger legal protections and stricter regulatory enforcement, while others emphasize the need for technological solutions such as encryption, decentralized data storage, and enhanced cybersecurity measures. At the same time, questions about how to strike a balance between digital innovation and individual privacy remain open-ended. The extent to which privacy rights can be safeguarded in an increasingly data-driven world is still a matter of ongoing research, debate, and policy development.

As digital interactions become more deeply integrated into daily life, the conversation around privacy remains as relevant as ever. Examining the implications of data collection, regulatory challenges, and the evolving nature of online surveillance may provide insights into how privacy frameworks will be shaped in the future. However, with technology advancing at an unprecedented rate, the question remains: how can individuals, governments, and corporations navigate this shifting landscape while ensuring that privacy remains a protected and enforceable right?

RIGHT TO PRIVACY

THE RIGHT TO PRIVACY IN INDIA

Privacy, as a concept, has long been regarded as an essential aspect of individual autonomy and personal freedom, it is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination, if we look at the Indian context of right to privacy, *The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. In the historic judgement of Justice K.S. Puttaswamy vs Union of India of 2017*

states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation." This provision firmly establishes privacy as an inviolable human right, safeguarded against arbitrary intrusions. While recognizing privacy as fundamental, the judgment also highlighted the need for balanced regulation, acknowledging that privacy, like other rights, is not absolute and may be subject to reasonable restrictions. It stated that any limitation on the right to privacy should satisfy the triple test of legality, necessity and proportionality .Another *PUCL vs Union of India* of 1997, commonly referred to as the telephone tapping cases. Here, the Supreme Court unequivocally recognized individuals' privacy interests in the content of their telephone communications, further reinforcing the acknowledgment of privacy rights within the ambit of Constitution These judgements have laid a robust foundation for safeguarding privacy rights against encroachments by both state and non-state entities, ensuring that individuals' privacy interests are duly respected and upheld.

RIGHT TO PRIVACY AT THE GLOBAL LEVEL

As far as we talk about the international front on privacy rights was first recognized by article 12 of The Universal Declaration of Human Rights, 1948 (UDHR). Which states that *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* Privacy is foundational to who we are as human beings, and every day, it helps us define our relationships with the outside world. It gives us space to be ourselves free of judgement and allows us to think freely without discrimination. It gives us the freedom of autonomy, and to live in dignity.

Privacy is also a right that enables our enjoyment of other rights, and interference with our privacy often provides the gateway to the violation of the rest of our rights. Forms of mass surveillance used today by governments directly threaten the very core of our right to privacy, as protected by Article 12 of the Universal Declaration of Human Rights as well as other human rights instruments.

.The International Covenant on Civil and Political Rights (ICCPR) has also enshrined it the article 17 that *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.2. Everyone has the right to the protection of the law against such interference or*

attacks. The recognition and protection of privacy in both the UDHR and the ICCPR highlight the United Nations' commitment to upholding human dignity, autonomy, and freedom worldwide. By explicitly acknowledging privacy as a fundamental aspect of human rights, these international instruments underscore the importance of personal autonomy, confidentiality, and protection from unwarranted interference in private affairs. In essence, the inclusion of privacy rights in the UDHR and the ICCPR reflects a collective endeavour to uphold individuals' rights to privacy as essential components of a just and equitable society.

THE RELEVANCE OF THE INTERNET TO THE RIGHT TO PRIVACY

The advent of internet and digitalisation where the role of internet has significantly taken over the world, the indulgence of the internet has reached to an exceptionally indivisible stage. Due to the culmination of internet, now privacy is not limited to affairs such as personal liberty, family, home, correspondence, etc which do not particularly hold the relevance with the internet. The privacy infringement, Unauthorized Access & hacking, identity-theft, phishing & social engineering, cyberstalking & online harassment, data theft, financial frauds & online scams, ransomware attacks, child exploitation & CSAM. In the digital age, privacy as a fundamental human right is increasingly threatened. The collection and storage of personal data by technology corporations and governments present substantial threats to individual privacy. Instances of data breaches, cyberattacks, and the improper handling of personal information have the potential to result in identity theft, financial detriment, and psychological anguish. Protects human dignity and other value such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age. Privacy is associated with liberty, but it is also associated with privilege, with confidentiality, with nonconformity and dissent, with shame and embarrassment, with the deviant and the taboo, and with subterfuge and concealment. Individuals' right to privacy has been complicated with the emphasis on security and the numerous developments in surveillance and information technology.

THE PRIVACY AND DATA PROTECTION ACTS-

LAWS IN INDIA-

THE DIGITAL PERSONAL DATA PROTECTION RULES 2023-

However, the laws or statutes regulating the digital affairs are still not sufficiently implemented

in India or the other several countries, talking about the existing laws India has recently drafted the Digital Personal Data Protection Rules, released by the Ministry of Electronics and Information Technology (MeitY) on January 3, 2025, aim to operationalize the Digital Personal Data Protection Act, 2023. These rules emphasize a citizen-centric approach, ensuring informed consent and granting individuals rights to access, correct, update, and erase their data. They also mandate verifiable parental consent for processing children's data under 18, with certain sector-specific exemptions. The draft introduces a principles-based framework to simplify notice and consent mechanisms, reducing "consent fatigue" among users. Additionally, the rules outline the registration and obligations of Consent Managers, entities that assist individuals in managing their data consents. To enhance accessibility, the draft is crafted using the SARAL framework, focusing on simple language and contextual definitions. MeitY has invited public feedback on these rules until February 18, 2025 underscoring the Indian governments to address the digital and privacy corncerns. An initial version was prepared by a committee of experts and circulated for public feedback in 2018. This was followed by the government's version of the bill that was introduced in Parliament in 2019—the Personal Data Protection Bill, 2019. This version was studied by a parliamentary committee that published its report in December 2021.[5] The government, however, withdrew this bill, and in November 2022, published a fresh draft for public consultations—the draft Digital Personal Data Protection Bill, 2022. This draft was quite different compared to the previous versions. The 2023 law is based, in significant part, on this draft. Notably, These four drafts were preceded by a landmark 2017 judgment by India's Supreme Court in *Justice K.S. Puttaswamy and Anr. v. Union of India and Ors.* The judgment declared that the right to privacy is part of the fundamental right to life in India and that the right to informational privacy is part of this right. The judgment, however, did not describe the specific contours of the right to informational privacy, and it also did not lay down specific mechanisms through which this right was to be protected.

THE INFORMATION TECHNOLOGY ACT 2000 -

The **Information Technology (IT) Act, 2000**, India's primary law governing cyber activities, includes provisions related to **privacy and data protection**, though it was not originally designed as a comprehensive privacy law.

Notably, **Section 43A** of the Act mandates that organizations handling **sensitive personal data**

must implement reasonable security practices, holding them liable for negligence in case of a data breach. Additionally, **Section 72** penalizes unauthorized access, disclosure, or leakage of personal data obtained in the course of official duties, reinforcing privacy protection. The **IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, framed under this Act, provide additional guidance on the lawful handling of personal data by companies.

However, the IT Act **lacks an explicit right to privacy**, which led to the introduction of the **Digital Personal Data Protection Act, 2023**, aiming to provide a more structured framework for privacy rights and data protection in India.

THE INTERNATIONAL LEGAL FRAMEWORK

The international laws In terms of existing frameworks, the **European Union's (EU)** 2016 *General Data Protection Regulation (GDPR)* is the most recent example of comprehensive regulation of data protection and privacy, setting a new threshold for international good practices. Building upon existing principles (e.g., the OECD Privacy Principles), it has become an important reference point for global work in this area. Article 5 of the GDPR, enshrines the core principles described above, requiring that personal data collection, storage, and use be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data.

Likewise, Several countries have established independent regulatory bodies to oversee data protection and privacy. **Estonia's Data Protection Inspectorate** (1999) ensures compliance

with laws like the Data Protection Act and safeguards constitutional rights, including access to personal data and privacy in family life. **South Africa's Information Regulator**, created under the Protection of Personal Information Act (2013), is accountable to the National Assembly and oversees compliance, public education, mediation, and cross-border cooperation. **The Philippines' National Privacy Commission**, formed under the Data Privacy Act (2012), monitors compliance, investigates complaints, and advises on privacy laws. **The UK's Information Commissioner's Office (ICO)**, originally introduced under the Data Protection Act 1984 and expanded by subsequent laws, enforces privacy regulations and reports to Parliament. These bodies play a crucial role in upholding data protection and privacy rights globally.

THE THREAT TO PRIVACY THROUGH DIGITAL CRIMES

PRIVACY-BASED CRIMES ON THE INTERNET

The rapid expansion of the internet has revolutionized communication, commerce, and information sharing. However, it has also given rise to **serious privacy-based crimes**, where personal data is exploited for malicious purposes. In an era where digital footprints are nearly impossible to erase, cybercriminals, corporations, and even government agencies have found ways to collect, misuse, and weaponize personal information, often without user consent.

One of the most common and damaging privacy-related crimes is **identity theft**, where cybercriminals steal personal details such as names, addresses, banking information, or social security numbers to commit fraud, make unauthorized purchases, or even impersonate individuals. **Phishing scams**, another widespread cyber threat, deceive users into providing sensitive data by posing as legitimate sources like banks, social media platforms, or government agencies. These scams are often carried out through emails, fake websites, or even messages, leading to financial losses and compromised accounts.

Another alarming issue is **unauthorized data collection and surveillance**. Many websites and applications track user activity, often without explicit consent, harvesting personal data for targeted advertising, political profiling, or even mass surveillance. This raises significant ethical concerns, as individuals lose control over their digital identities and private communications. In some cases, governments have been accused of monitoring citizens under the guise of national security, blurring the lines between lawful oversight and privacy

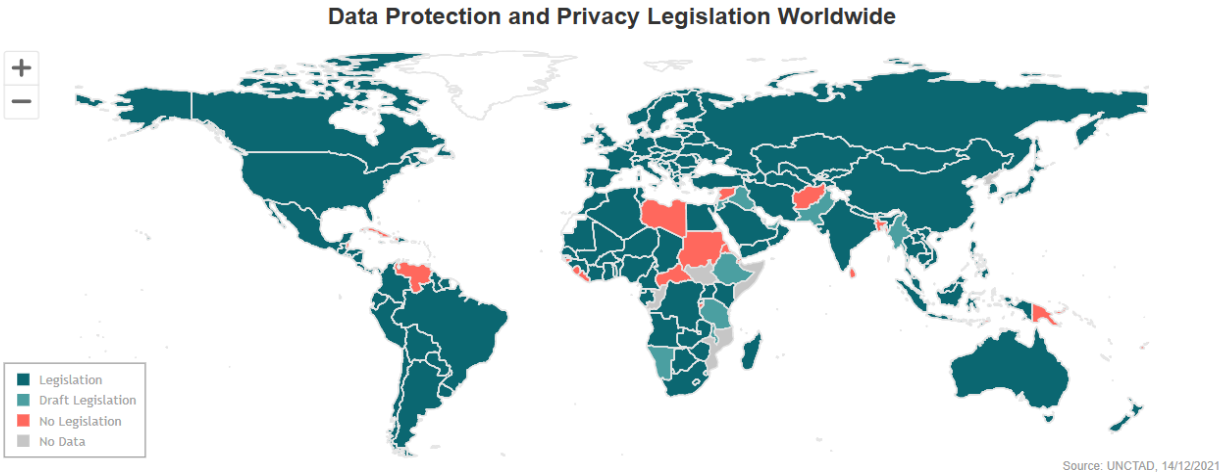
violations.

Hacking and large-scale data breaches have also become a recurring threat, exposing millions of users' private information. Cybercriminals infiltrate corporate databases, government records, and even healthcare institutions, leaking sensitive details such as financial transactions, medical histories, and private conversations. These breaches not only affect individuals but also businesses and governments, leading to significant economic and reputational damage.

Emerging privacy violations like **doxxing**, where an individual's private information is publicly exposed to harass or threaten them, and **CSAM (Child Sexual Abuse Material) distribution**, which exploits minors and spreads illicit content, further underscore the dark side of internet anonymity. Additionally, **revenge porn and deepfake technology** have been misused to violate personal privacy by creating and sharing explicit content without consent, causing severe emotional and psychological harm to victims.

As technology continues to evolve, so do the methods used to exploit personal data. With the increasing reliance on digital platforms, **ensuring privacy and data protection** has become more critical than ever. Stronger legal frameworks, enhanced cybersecurity measures, ethical corporate practices, and public awareness are necessary to combat these crimes and safeguard individual privacy in an increasingly interconnected world.

STATISTICS EXPLAINING:DATA PROTECTION ACTS IMPLEMENTATION AND THE PRIVACY BASED CRIMES-



Asia-Pacific (60 countries)

Countries with legislation

Legislation:
34 (57%)

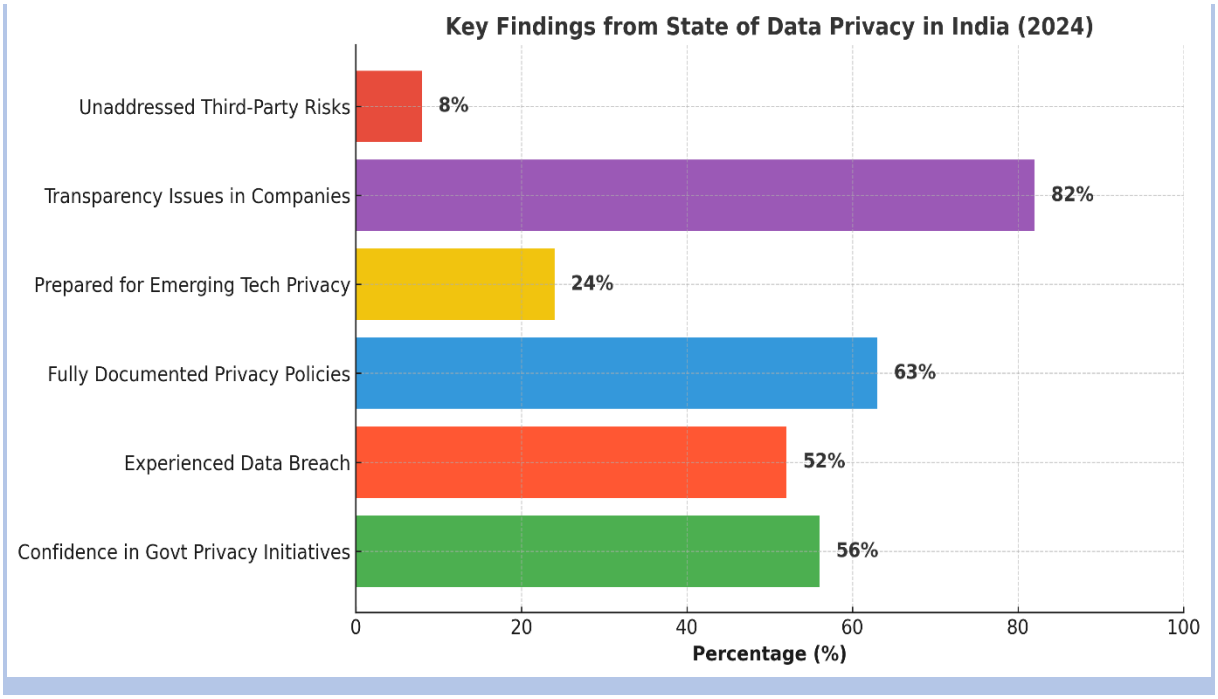
Draft Legislation:
7 (12%)

No Legislation:
15 (25%)

No Data:
4 (7%)

137 out of 194 countries had put in place legislation to secure the protection of data and privacy.

FOLLOWING DATA DEPICTS THE STATE OF DATA PRIVACY IN INDIA SURVEY REPORT 2024 EXAMINES THE CURRENT PRIVACY LANDSCAPE IN INDIA, FOCUSING ON THE COMPLIANCE, CHALLENGES, AND TRENDS IN DATA PROTECTION



THE FUTURE OF PRIVACY AND ADVENT OF AI-

WHAT IS AI PRIVACY AND PRACTICE-

AI privacy refers to the practice of protecting personal or sensitive information that artificial intelligence systems collect, process, share, or store. It is a critical aspect of modern digital governance, ensuring that individuals' data remains secure and used ethically. AI privacy is deeply intertwined with data privacy, also known as information privacy, which grants individuals control over how their personal information is collected, stored, and utilized by organizations. But the concept of data privacy predates AI and how people think of data privacy has evolved with the advent of AI.

Although the concept of data privacy existed long before AI, the rapid advancement of artificial intelligence has significantly reshaped its scope and implications. AI-driven technologies, such as machine learning algorithms and deep learning models, process vast amounts of data to enhance decision-making and predictive capabilities. However, this reliance on extensive data

collection raises concerns about unauthorized access, biased data processing, and potential misuse.

With AI's ability to analyze and infer sensitive details, ensuring strong privacy safeguards is essential, there are greater risks with the rising technology.

CASE STUDIES SHOWCASING THE DATA INFRINGEMNT -

1. THE CAMBRIDGE ANALYTICA CASE -

The Cambridge Analytica scandal remains one of the most significant examples of AI-driven privacy breaches, demonstrating the risks associated with unethical data collection and misuse. The political consulting firm Cambridge Analytica illicitly obtained personal data from over 87 million Facebook users without their explicit consent, leveraging a seemingly innocuous personality quiz application. This application not only collected data from users who participated but also accessed information from their social network, exponentially expanding the dataset.

Through AI-powered psychological profiling techniques, the harvested data was utilized to construct detailed personality models of users. These profiles were subsequently employed for micro-targeting political advertisements, particularly during the 2016 U.S. Presidential Election. The incident underscored the capability of AI to derive highly sensitive personal insights—such as political affiliations and behavioral tendencies—from ostensibly benign online activities, including Facebook likes, interactions, and browsing behavior.

This case highlighted the ethical and regulatory challenges posed by AI-driven data analytics, wherein information collected for one purpose was repurposed for another, violating fundamental privacy principles. In response, global policymakers intensified efforts to strengthen data protection regulations, exemplified by the enactment of the General Data Protection Regulation (GDPR) in Europe and increased scrutiny of major technology corporations' data governance practices. The scandal served as a catalyst for enhanced transparency, accountability, and regulatory oversight in the field of AI and data privacy.

2. STRAVA HEATMAP CASE

The Strava Heatmap Incident (2018) exposed a significant privacy breach caused by the app's

default data-sharing settings. Strava, a fitness-tracking application, released a Global Heatmap showcasing user activity routes worldwide. While the feature aimed to create a global network of athletes, it unintentionally revealed sensitive military locations, including undisclosed U.S. bases, patrol routes, and high-security government facilities.

The heatmap, built using GPS data from millions of users, displayed movement patterns in remote areas where civilian activity was minimal, making military sites easily identifiable. Analysts discovered base perimeters, supply routes, and patrol paths, raising concerns that adversaries could track troop movements and security protocols. Many military personnel had unknowingly contributed to the heatmap, as Strava's default settings enabled public data sharing without explicit user awareness.

Following public scrutiny, Strava responded by enhancing privacy controls and making it easier for users to opt out of data sharing. However, the incident underscored how AI-driven data aggregation, even when anonymized, can inadvertently compromise security. It served as a wake-up call for organizations handling sensitive geolocation data, highlighting the need for stronger default privacy settings and clearer user awareness.

With the rapid advancement of AI technology, the role of regulators in enacting comprehensive privacy legislation has become more crucial than ever. As AI continues to evolve, regulatory frameworks must strike a balance between protecting individual privacy and encouraging technological innovation. Given the vast amount of personal data AI systems process, privacy laws must establish clear guidelines on data collection, usage, and security to mitigate risks associated with data misuse.

Future regulations could impose restrictions on the types of data AI tools are permitted to collect and process, ensuring that sensitive personal information remains protected. Additionally, companies deploying AI-driven technologies may be required to maintain transparency in their data-handling practices, including disclosing how data is gathered, stored, shared, and utilized. In cases of privacy violations or data breaches, regulatory frameworks could introduce strict penalties to hold organizations accountable and encourage stronger cybersecurity measures. Given the fast-paced evolution of AI, legislators must ensure that privacy laws are adaptable and future-proof. This means designing flexible regulatory structures that can evolve alongside technological advancements without becoming obsolete. An effective legal framework should incorporate continuous review mechanisms, allowing

policymakers to make timely adjustments in response to emerging AI capabilities and potential threats to data privacy. By implementing robust yet adaptable regulations, governments can protect individuals' rights while fostering responsible AI innovation in an increasingly data-driven world.

THE ADVENT OF AI -

Artificial intelligence is evolving rapidly and has become a transformative force in today's technological landscape. It enhances decision-making processes, revolutionizes industries, and improves lives. With projections estimating AI's contribution to the global economy at a staggering $15.7 trillion by 2030, it is evident that this technology is here to stay. However, alongside its numerous advantages, AI also brings forth significant challenges that require human oversight and innovative problem-solving.

As AI advances, the complexity of issues spanning technological, ethical, and social dimensions continues to grow. Some of the most pressing challenges in 2024 include concerns over privacy and data protection, algorithmic bias, transparency, and the socio-economic impact of job displacement. Addressing these challenges requires interdisciplinary collaboration and the formulation of regulatory policies. While AI offers incredible benefits, it also raises cybersecurity and ethical concerns, highlighting the need for a balanced and holistic approach that maximizes its advantages while mitigating risks.

PRIVACY BASED CHALLENGES DUE TO AI

1. Ethical Concerns in AI

Ethics in AI is a crucial issue that must be addressed, as it encompasses concerns related to privacy, bias, and social impact. AI-driven surveillance systems pose significant privacy risks, while its deployment in sensitive areas such as healthcare and criminal justice necessitates the application of ethical principles to ensure fair and unbiased outcomes. Striking a balance between technological advancement and ethical integrity is essential to prevent violations of human rights and promote responsible AI development.

2. Bias in AI Systems

AI bias arises when machine learning algorithms replicate and amplify the biases present

in training datasets. If data used for training AI models is biased, the system inherits and reinforces these biases, potentially leading to unfair treatment in areas such as hiring, law enforcement, and loan approvals. To mitigate this, AI developers must adopt rigorous data selection processes, implement bias-reducing preprocessing techniques, and design algorithms that promote fairness and equity.

3. Integration of AI into Existing Systems

Implementing AI within current systems can be a challenging process, requiring organizations to identify suitable application areas, fine-tune AI models, and ensure seamless integration with existing workflows. Collaboration between AI experts and domain specialists is essential for optimizing solutions and addressing challenges related to data interoperability and personnel training. Successful AI integration necessitates strategic planning, stakeholder involvement, and phased implementation to enhance operational efficiency and drive innovation.

4. Computing Power and Infrastructure Demands

AI models, particularly those involving deep learning, require substantial computing power. The need for high-performance hardware such as GPUs and TPUs significantly increases operational costs and energy consumption, making it difficult for smaller organizations to keep up. Innovations in hardware architecture, including neuromorphic and quantum computing, offer potential solutions. Additionally, leveraging distributed computing and cloud-based services can help overcome computational limitations while maintaining efficiency and sustainability.

5. Data Privacy and Security Risks

AI systems rely on vast amounts of data, making data privacy and security a critical concern. Ensuring the confidentiality, integrity, and availability of data is essential to prevent breaches, leaks, and unauthorized access. Robust encryption techniques, data anonymization, and adherence to stringent data protection regulations are necessary to maintain trust and compliance. Moreover, privacy-preserving approaches such as differential privacy and federated learning can help minimize privacy risks while retaining data utility. Transparent data governance and ethical handling of user data are

essential to fostering public confidence in AI systems.

6. **Legal and Regulatory Challenges**

   The legal landscape surrounding AI is still evolving, with key concerns including liability, intellectual property rights, and regulatory compliance. Questions of accountability arise when AI-driven decisions result in errors, system failures, or harm. Additionally, copyright disputes emerge over AI-generated content and algorithmic ownership. To address these legal challenges, collaboration between legal professionals, policymakers, and technology experts is crucial in establishing clear regulations that balance innovation with accountability and protect stakeholders' rights.

Addressing these challenges requires a concerted effort from governments, industries, and research institutions to ensure that AI development is ethical, secure, and beneficial for all. By prioritizing transparency, fairness, and responsible innovation, society can harness AI's full potential while mitigating its associated risks.

THE ROLE OF GOVERNMENT AND PUBLIC AWARENESS PROGRAMMES FOR THE BREAKTHROUGH-

SOLUTIONS AND POLICIES- THE INDIAN CONTEXT

The Indian government has implemented several initiatives to strengthen data privacy and protection. One of the key measures includes the establishment of a comprehensive privacy governance and compliance framework, which encourages organizations to enhance governance, risk, and compliance (GRC) strategies while promoting the adoption of privacy-enhancing technologies and third-party risk management. Additionally, the government has enforced data localization policies and restrictions on cross-border data transfers, ensuring that critical personal data is stored within the country. For example, the Reserve Bank of India (RBI) mandates that financial data must be stored exclusively in India. To further support these efforts, industry collaborations such as those led by the Confederation of Indian Industry (CII) and the Centre for Digital Transformation (CDT) focus on capacity building through cybersecurity masterclasses, privacy management training, and awareness programs on data security and regulatory compliance. Public awareness initiatives also play a crucial role in strengthening data protection, with organizations being encouraged to disclose their data

collection and processing methods transparently while raising awareness about consumer data rights and consent. Furthermore, businesses are being guided to establish dedicated privacy teams, implement automation in data governance, and develop strong privacy rights management programs. These collective efforts aim to create a secure digital ecosystem where data protection is prioritized, risks are mitigated, and both organizations and individuals are equipped to handle privacy challenges effectively.

CATERING THE PUBLIC -

Public awareness initiatives play a crucial role in strengthening data privacy and protection in India. Industry-led efforts, such as those by the Confederation of Indian Industry (CII) and the Centre for Digital Transformation (CDT), focus on training programs, cybersecurity masterclasses, and privacy management workshops to enhance digital literacy and regulatory compliance. Organizations are encouraged to adopt transparent data handling practices, ensuring that individuals are well-informed about how their personal data is collected, processed, and shared. Efforts are also being made to educate consumers about their data rights and the importance of giving informed consent before sharing personal information. Additionally, businesses are being guided to implement automation in data governance, develop dedicated privacy teams, and strengthen privacy rights management programs. These measures collectively aim to build a culture of data protection, where both individuals and organizations are aware of their roles in safeguarding personal information and ensuring compliance with privacy standards.

THE SUGGESTIONS WHICH COULD BE CARRIED OUT TO BRING THE CHANGE-

To strengthen data privacy and protection at a global level, several key suggestions need to be implemented:

1. **Harmonization of Data Privacy Laws** – Countries should work towards aligning their data protection regulations, such as GDPR, CCPA, and similar frameworks, to establish uniform global standards. This would facilitate cross-border data transfers while ensuring privacy rights are protected consistently worldwide.

2. **Global Data Protection Treaty** – There is a need for an international agreement that

sets minimum data privacy standards, ensuring accountability and compliance across nations. Such a treaty should define data sovereignty, lawful processing conditions, and enforcement mechanisms.

3. **Stronger Enforcement Mechanisms** – Global collaboration among regulatory bodies should be strengthened to enforce data protection laws effectively. This includes establishing international privacy task forces that can investigate cross-border violations and impose penalties on non-compliant entities.

4. **Privacy by Design and Default** – Organizations worldwide should be required to integrate privacy into technology development from the outset. This includes implementing strong encryption, secure data storage, and minimal data collection policies to protect user information.

5. **Cybersecurity Enhancement and Incident Reporting** – Governments and businesses should adopt stricter cybersecurity measures, including mandatory incident reporting for data breaches. A centralized global database for breach notifications can help track and prevent large-scale cyber threats.

6. **Greater Consumer Awareness and Digital Literacy** – Governments and private entities should invest in public education campaigns to inform individuals about their data rights, online privacy risks, and best practices for protecting personal information. Training programs should be integrated into schools, workplaces, and public initiatives.

7. **Accountability for Tech Giants and Corporations** – Major technology firms that collect vast amounts of personal data should be subject to stricter regulations and independent audits to ensure ethical data practices. They should also be required to offer transparent data policies and provide users with greater control over their information.

8. **Ethical AI and Data Usage Guidelines** – With the rise of artificial intelligence, clear guidelines must be established to prevent misuse of personal data in AI-driven technologies. This includes ensuring AI systems are transparent, accountable, and do not lead to biased or discriminatory outcomes.

9. **Secure and Ethical Cross-Border Data Transfers** – Governments should create agreements that allow the safe and lawful transfer of data between nations without

compromising privacy. Mechanisms like the EU-U.S. Data Privacy Framework should be improved and expanded globally.

10. **Incentives for Privacy Innovation** – Governments should encourage businesses and tech companies to develop privacy-enhancing technologies (PETs) such as decentralized identity systems, encrypted messaging platforms, and data anonymization tools by providing funding, tax incentives, or regulatory support.

By implementing these measures, the global community can build a more secure, transparent, and privacy-focused digital environment that protects individuals' rights while enabling technological growth and innovation.

FACTORS WHICH INFLUENCE RIGHT TO PRIVACY AT LARGER LEVEL -

The right to privacy is a fundamental human right that is increasingly under threat in the digital age due to various technological advancements. Social media platforms, while fostering connectivity, encourage users to share personal details, often without full awareness of how their data is collected, analyzed, and monetized. This compromises their privacy by enabling targeted advertising, profiling, and potential misuse of personal information. Similarly, the rapid expansion of the Internet of Things (IoT) has introduced devices that continuously collect user data, often lacking adequate security measures, leading to unauthorized surveillance and data breaches. Online tracking mechanisms, including cookies and behavioral analytics, further erode privacy by allowing corporations to monitor and profile users without explicit consent. The widespread use of public Wi-Fi networks also jeopardizes personal privacy, as unsecured connections expose sensitive information to cybercriminals who can exploit such vulnerabilities for identity theft and financial fraud.

Cloud computing, while providing convenient data storage solutions, presents another privacy challenge, as sensitive data stored on remote servers is susceptible to breaches and unauthorized access. The growing adoption of facial recognition technology raises serious concerns regarding mass surveillance and biometric data misuse, posing a direct threat to an individual's right to anonymity and freedom of movement. Additionally, artificial intelligence (AI) and big data analytics process vast amounts of personal information to predict behavior and make automated decisions, often without transparency, leading to biased outcomes and discrimination in critical areas such as employment and financial services. These developments

highlight the urgent need for robust data protection laws, ethical AI regulations, and stronger cybersecurity measures to uphold the right to privacy. As technology continues to evolve, it is crucial for individuals, corporations, and governments to work collectively to establish legal safeguards, promote transparency, and empower users with greater control over their personal data, ensuring that the right to privacy remains protected in the digital era.

THE TECHNIQUES LINKED WITH PRIVACY AND DIGITAL OPERATIONS - ENCRYPTION

At its most basic level, encryption is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it. That process can range from very simple to very complex, and mathematicians and computer scientists have invented specific forms of encryption that are used to protect information and data that consumers and businesses rely on every day.

Encryption works by encoding "plaintext" into "ciphertext," typically through the use of cryptographic mathematical models known as algorithms. To decode the data back to plaintext requires the use of a decryption key, a string of numbers or a password also created by an algorithm. Secure encryption methods have such a large number of cryptographic keys that an unauthorized person can neither guess which one is correct, nor use a computer to easily calculate the correct string of characters by trying every potential combination (known as a brute force attack).

Types of Encryption

The most common types of encryption algorithms are symmetric and asymmetric.

Symmetric encryption, also known as a shared key or private key algorithm, uses the same key for encryption and decryption. Symmetric key ciphers are considered less expensive to produce and do not take as much computing power to encrypt and decrypt, meaning there is less of delay in decoding the data.

The drawback is that if an unauthorized person gets their hands on the key, they will be able to decrypt any messages and data sent between the parties. As such, the transfer of the shared key needs to be encrypted with a different cryptographic key, leading to a cycle of dependency.

Asymmetric encryption, also known as public-key cryptography, uses two separate keys to encrypt and decrypt data. One is a public key shared among all parties for encryption. Anyone with the public key can then send an encrypted message, but only the holders of the second, private key can decrypt the message.

Asymmetric encryption is considered more expensive to produce and takes more computing power to decrypt as the public encryption key is often large, between 1,024 and 2,048 bits. As such, asymmetric encryption is often not suited for large packets of data.

End-to-End Encryption (E2EE): Ensures that only the sender and recipient can read messages (e.g., WhatsApp, Signal).

ANONYMIZATION

Anonymization is a data protection technique that removes or alters personal identifiers from datasets to prevent individuals from being identified. This method is used to comply with privacy laws such as the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection (DPDP) Act, 2023 while still allowing organizations to analyze data without violating user privacy.

Techniques of Anonymization

-Data Masking: Hides specific parts of personal data (e.g., displaying only the last four digits of a credit card number).

Pseudonymization: Replaces private identifiers with unique but non-identifiable symbols (e.g., replacing names with random numbers). Generalization: Reduces the precision of data (e.g., replacing exact ages with age ranges like 20-30). Differential Privacy: Adds statistical noise to datasets to prevent the re-identification of individuals.

Applications of Anonymization; Healthcare Data Protection – Hospitals anonymize patient data before sharing it for medical research. Marketing Analytics – Companies use anonymized browsing data to improve their services without tracking individuals. Government and Census Data – Authorities anonymize census data to conduct demographic analysis without compromising individual privacy.

TERMS TO BE OBSERVED IN THE CONTEXT OF PRIVACY-

Two of the most pressing privacy concerns in the modern world are Digital surveillance and data exploitation:

Digital surveillance has become one of the most pressing privacy concerns in the modern world. The rapid advancement of technology has enabled governments, corporations, and cybercriminals to collect, analyze, and utilize personal data, often without explicit user consent. While surveillance is often justified for security and law enforcement purposes, it can also be misused for mass monitoring, political control, and commercial gain. Governments employ surveillance tools such as CCTV cameras, facial recognition, and internet tracking to monitor individuals' activities, raising concerns about mass data collection and the erosion of civil liberties. Additionally, mobile phone tracking and AI-based surveillance further intensify the privacy risks, as they enable authorities and private entities to track movements, behaviors, and personal interactions in real time. Such practices not only compromise personal freedoms but also pose the risk of data breaches and unauthorized access to sensitive information.

Simultaneously, **data exploitation** has become a widespread issue as corporations collect vast amounts of user information through digital platforms, often for commercial purposes. Social media companies, e-commerce platforms, and online services track browsing habits, purchasing behavior, and even biometric data to tailor advertisements, manipulate consumer behavior, and maximize profits. Data brokerage has further exacerbated the problem, with third-party firms buying, aggregating, and selling personal data without the explicit knowledge of users. The misuse of data has also been evident in political campaigns, where organizations have leveraged psychological profiling and targeted advertising to influence public opinion, as seen in the Cambridge Analytica scandal. Moreover, AI-driven decision-making based on data profiling can lead to discriminatory practices in hiring, lending, and insurance approvals, disproportionately affecting marginalized groups. Cybercriminals, too, exploit personal data through hacking, identity theft, and financial fraud, exposing individuals to severe risks.

The implications of digital surveillance and data exploitation are profound, leading to a loss of trust in online platforms, manipulation of consumer and political choices, and potential threats to democracy. Legal frameworks such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and India’s Digital Personal Data Protection (DPDP) Act, 2023 have been introduced to regulate

data collection and provide individuals with more control over their personal information. However, stronger measures are required to address emerging privacy threats. Governments must enforce stricter data protection laws, ensure transparency in data collection, and place restrictions on mass surveillance. Organizations must adopt ethical AI practices, disclose their data collection policies, and implement robust cybersecurity measures. Individuals can also take steps to protect their privacy by using encrypted communication tools, enabling privacy settings, utilizing VPNs and privacy-focused browsers, and limiting data sharing on digital platforms.

The future of privacy depends on a **balanced approach that safeguards security while protecting fundamental rights**. Unchecked surveillance threatens personal freedoms, while unregulated data exploitation fuels unethical corporate practices and increases the risk of cybersecurity breaches. By strengthening privacy regulations, promoting transparency, and raising awareness, society can ensure that digital advancements serve humanity without compromising the fundamental right to privacy.

CONCLUSION

In an era where data has become the new currency, the right to privacy is under unprecedented threat. The rapid advancement of digital technologies has enabled governments, corporations, and cybercriminals to collect, monitor, and exploit personal information on a massive scale, often without individuals' explicit consent. From social media tracking, AI-driven profiling, and IoT surveillance to state-sponsored digital monitoring and cybercrime, privacy risks have become deeply embedded in modern life. The rise of facial recognition, biometric authentication, and behavioral data analysis further complicates the situation, making it easier to track individuals and predict their actions. While these innovations offer convenience and security in some areas, they also present significant risks of data misuse, discrimination, and loss of autonomy. The increasing reliance on digital platforms has blurred the line between public and private spaces, often leaving individuals vulnerable to mass surveillance and commercial exploitation.

Despite these challenges, global efforts to protect privacy have gained momentum. Regulatory frameworks such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the U.S., and India's Digital Personal Data Protection (DPDP) Act, 2023 have been introduced to safeguard individuals' personal

information. These laws focus on data minimization, consent-based processing, and transparency, aiming to give users greater control over how their information is collected and used. However, legislation alone is not enough. The effectiveness of these regulations depends on strict enforcement, continuous technological updates, and a commitment from both governments and businesses to prioritize privacy over profit. Many companies still engage in aggressive data collection practices, and loopholes in existing laws allow for continued exploitation of personal information. Stronger accountability measures, independent oversight bodies, and heavy penalties for data breaches are necessary to deter unethical data practices and reinforce privacy protections.

At the same time, the responsibility to protect privacy does not lie solely with governments and corporations—individuals must also take proactive measures. Digital literacy and awareness are crucial in helping people understand the implications of their online behavior. Using privacy-enhancing technologies such as encryption, anonymization, virtual private networks (VPNs), and secure communication platforms can help individuals safeguard their personal data. Avoiding oversharing on social media, regularly reviewing privacy settings, and being cautious about data-sharing agreements are small but effective steps in protecting personal information from exploitation.

Furthermore, corporations and technology developers must adopt ethical data practices, ensuring that privacy is integrated into the very design of digital products and services. The concept of Privacy by Design (PbD) should be at the core of innovation, ensuring that personal data is collected minimally, stored securely, and processed responsibly. The role of artificial intelligence (AI) in data processing and decision-making also requires stricter oversight to prevent bias, discrimination, and opaque decision-making systems. Businesses must be held accountable for how they handle user data, and clear regulations must be in place to prevent AI from being used for unethical purposes such as manipulation, surveillance, or unfair profiling.

Ultimately, privacy is more than just a legal right—it is a fundamental pillar of human dignity, security, and freedom. The erosion of privacy leads to a world where individuals are constantly monitored, manipulated, and vulnerable to exploitation. As digital technologies continue to advance, the need to proactively defend and strengthen privacy protections has never been more urgent. The future of privacy depends on collective responsibility— from individuals

taking charge of their digital footprints to policymakers enforcing stricter regulations and corporations committing to ethical data practices. Without immediate action, privacy could become a privilege rather than a right, accessible only to those who can afford the tools and resources to protect themselves.

The time to act is now. Governments, corporations, and individuals must work together to create a digital ecosystem where privacy is respected, protected, and upheld as a fundamental human right. Strengthening privacy laws, promoting ethical technology development, and empowering individuals with knowledge and tools to safeguard their personal information is the only way forward. If we do not act decisively today, we risk a future where privacy is no longer a choice, but a luxury that only a few can afford.

REFERENCES

Online Articles & Reports

Manupatra. (n.d.). *Right to privacy in digital age*. Retrieved from https://articles.manupatra.com/article-details/Right-to-Privacy-in-Digital-Age

Supreme Court Observer. (n.d.). *Puttaswamy v. Union of India: Fundamental right to privacy case background*. Retrieved from https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/

Indian Kanoon. (n.d.). *Justice K.S. Puttaswamy (Retd.) vs. Union of India & Ors.* Retrieved from https://indiankanoon.org/doc/127517806/

Indian Kanoon. (n.d.). *Puttaswamy judgment on Aadhaar*. Retrieved from https://indiankanoon.org/doc/31276692/

Press Information Bureau (PIB). (2024). *Press release on data protection*. Retrieved from https://pib.gov.in/PressReleasePage.aspx?PRID=2090271

MyGov India. (2025). *Draft DPDP Rules 2025*. Retrieved from https://innovateindia.mygov.in/dpdp-rules-2025/

Ministry of Electronics and Information Technology (MeitY). (n.d.). *Rules for Information Technology Act, 2000*. Retrieved from https://www.meity.gov.in/documents/act-and-policies/rules-for-information-technology-act-2000

United Nations. (n.d.). *Universal Declaration of Human Rights: Article 12*. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012

Office of the High Commissioner for Human Rights (OHCHR). (n.d.). *International Covenant on Civil and Political Rights*. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

General Data Protection Regulation (GDPR). (n.d.). *General Data Protection Regulation (GDPR) overview*. Retrieved from https://gdpr-info.eu/

United Nations Conference on Trade and Development (UNCTAD). (n.d.). *Data protection and privacy legislation worldwide*. Retrieved from https://unctad.org/page/data-protection-and-privacy-legislation-worldwide#:~:text=137%20out%20of%20194%20countries

Protiviti. (2024). *State of data privacy in India: Survey report 2024*. Retrieved from https://www.protiviti.com/sites/default/files/202408/state_of_data_privacy_in_india_survey_report_2024.pdf

IBM. (n.d.). *AI & privacy: Managing risks in the digital world*. Retrieved from https://www.ibm.com/think/insights/ai-privacy

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, April 4). *Cambridge Analytica scandal fallout*. The New York Times. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Hern, A. (2018, January 28). *Fitness tracking app gives away location of secret US army bases*. The Guardian. Retrieved from https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Google Cloud. (n.d.). *What is encryption?* Retrieved from https://cloud.google.com/learn/what-is-encryption

K2View. (n.d.). *Anonymization vs. encryption: Key differences*. Retrieved from https://www.k2view.com/blog/anonymization-vs-encryption/#:~:text=The%20anonymization%20of%20data%20provides

Fox Mandal. (n.d.). *Data protection ecosystem: Need to combat organized data exploitation*. Retrieved from https://www.foxmandal.in/data-protection-ecosystem-need-to-combat-organised-data-exploitation/