INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBERSECURITY LAWS AND AI: SAFEGUARDING IDENTITY IN AN ERA OF SMART SURVEILLANCE

AUTHOR – PRIYA* & DR. MOHIT KANWAR**, LL.M. (MASTER OF LAWS)* & ASSISTANT PROFESSOR**, UNIVERSITY INSTITUTE OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA.

BEST CITATION - PRIYA & DR. MOHIT KANWAR, CYBERSECURITY LAWS AND AI: SAFEGUARDING IDENTITY IN AN ERA OF SMART SURVEILLANCE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 466-479, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

With the explosion of AI Driven Smart Surveillance systems in the digital era, the integration of cybersecurity and AI has played a massive role in reshaping identity protection. With the progress of digitalization in India, these technologies strengthen our security by enhancing the power of real time monitoring and detecting threats, however it also creates new challenges for privacy and data security. In this thesis, India's existing cybersecurity framework, incorporating aspects of the 'Information Technology Act, 2000' and the 'Digital Personal Data Protection Act, 2023' (DPDPA), is studied, to locate gaps in regulating AI-driven surveillance, and its impact on identity protection. This research shows how AI frameworks in India can benefit from their comparison with international standards, e.g., GDPR, and their studies. The research stresses the demand for adaptive legal reforms that entail the clear data minimization practices, strict enforcement and privacy requirements. The results indicate that by taking cues from international best practices, India can experience the use of AI in cybersecurity without infringing on individual privacy rights. This research gives actionable insights to support a balance, ethically grounded framework that combines security and privacy to drive the field forward.

Keywords: Cybersecurity, Artificial Intelligence, Identity Protection, Smart Surveillance, Digital Personal Data Protection Act, GDPR, Privacy, Data Security, AI-driven Surveillance

INTRODUCTION

As our lives become more and more digitized, we have needed to advance simplified versions of cybersecurity and artificial intelligence (AI). The realm of cybersecurity has expanded beyond protecting organizations' systems from hacking, all the way to protecting individual identities as the internet becomes increasingly of our personal data. Such proportions of data breach and identity theft along with the growth of internet and data transactions have in turn become one of the identity related crimes that are being perpetrated in India, where cybercriminals are increasingly using advanced AI driven methods. While this new technology is making our lives easier in many ways, government and corporate entities are simultaneously deploying AI–powered surveillance systems to bolster security measures, creating what's been dubbed as "smart surveillance." However, these developments serve as the cause for legal, ethical, and privacy concerns, since although AI has improved the security level, it can also potentially pose a danger to personal privacy and data protection. When it comes to smart surveillance technology with Big Data, you need identity protection most of all: Typically, smart surveillance technologies process and store an incredible amount of personal data. In this digital world, we need informed and strong legal frameworks to provide a workable solution to cyber security and AI empowered surveillance. In this era of pervasive

surveillance, the challenges of balancing security and privacy rights are with legal systems, including India's ones. India has therefore witnessed the rise of several legal regulations in relation to cybersecurity and data protection, which are, nonetheless, always scorned as inadequate to the sophisticated digital threats. However, the onus falls on India to fully develop its legal discourse with respect to cybersecurity laws and AI since the identification of effective identity protection in the wake of rapidly advancing smart surveillance technologies has yet to be addressed. [740]

With the surveillance technology so prevalent in our time identity protection is a must. Governments and corporations employ surveillance technologies empowered by AI such as facial recognition systems, biometrics and algorithmic data monitoring for public security and to keep an eye on any illegal activities. Unfortunately, these tools regularly collect huge amounts of personal data, which can be inadvertently breached if not properly managed. While the employing of AI in surveillance also contributes to prescription of national security, it also poses the risk of unauthorized access to the personal sensitive information. Additionally, if not accompanied by proper regulatory oversight, such surveillance methods could be misused. This tension highlights the need for specific cybersecurity laws that cater not only to technological advancements but also to the fundamental right to privacy, as enshrined in *"Justice K.S. Puttaswamy v. Union of India"*[741], The right to privacy was born on these shores where it came under the purview of the Indian Supreme Court that recognized the accepted right to privacy as an intrinsic part of the right to life and liberty under Article 21 of the Indian Constitution. Barring the decision, India has reached a substantial forward step in its constitutional jurisprudence, but it remains to be seen by how the legal system is going to bend those rights against AI-based surveillance. Given these concerns, this research seeks to examine the existing legal frameworks governing cybersecurity in India, identify any gaps in these laws and examine whether these provisions will sufficiently cater to the problem of managing AI in ensuring identity protection when surveillance is at its highest.

Within the ambit of this study, the legal developments in India vis-a-vis cybersecurity, AI, and identity protection with respect to smart surveillance are also explored. The research also explores the effectiveness of India's important cybersecurity laws such as the 'Information Technology Act, 2000' and the 'Digital Personal Data Protection Act, 2023' with respect to data protection as a national and personal security matter. But both laws have been criticized for being too vague and for not being developed with an AI world in mind. The study also looks at international standards and best practices because India's cybersecurity laws are subject to greater scrutiny in relation to global benchmarks, including the European Union's 'General Data Protection Regulation' or GDPR, which has set an exemplary data privacy and protection standard. This study contributes to ongoing debate of privacy vs security by conducting such a critical examination of legal instruments on their effectivity to deal with unaccounted AI in cybersecurity and surveillance, further offering possible reflections on how Indian legal framework can evolve to handling AI's role in cybersecurity and surveillance within the law. [742]

This research seeks, first, to analyses the present cyber security laws of India in light of AI based surveillance systems and their effect on identity protection. Second, the study will also identify loopholes in these laws that compromise people's privacy. Second, this paper will examine the needed reform to

[740] Punit Bhatia and Eline Chivot, AI & Privacy: How to Find Balance 150 (Ek Advisory, Kindle Edition, 1st edn., 2021).
[741] (2017) 10 SCC 1.
[742] Ranadeep Reddy Palle and Krishna Chaitanya Rao Kathala, *Privacy in the Age of Innovation: AI Solutions for Information Security* 112 (Apress, Berkeley, CA, 1st edn., 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

develop a legal framework to protect individual identities while still mitigating the security concerns of these systems. The study also seeks to provide foresight into future legal challenges and considerations that lawmakers must deal with to promote privacy in this space as AI and surveillance technologies grow at an ever-increasing pace. Additionally, the study will point out that laws protecting data in the future must not only address the legal aspects, but also cover the application of AI to prevent abuse of people's rights.

In this study, I frame a couple of research questions which provide insight in the core issues on which cybersecurity, AI and identity protection in India is built upon. First and foremost, it tests the current laws of cybersecurity and data protection about whether they are properly equipped to protect the personal identity of people from the threats generated by AI. These laws do they cover the emerging threats posed by smart surveillance technologies, or are there critical gaps into which the citizens are going to be left vulnerable? Furthermore, the study will examine the suitability of India's legal system to embrace Progress in AI and Cyberlaw, by reviewing relevant statutes, judicial observations and latest reforms. What international lessons can be applied to India's data protection law, and how does it measure up to international standards? Finally, the research will evaluate the ethical considerations integral to AI for surveillance. More precisely, it aims to determine how Indian laws can be interpreted and refined to sanction for AI systems allowing misuse and safeguarding the perusal of individual rights in developing digital India. The study aims at answering these research questions so as to provide a well-rounded legal review of how India may reinforce its cybersecurity laws in securing identity in presence of increasing smart surveillance.

UNDERSTANDING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

In the present day connected digital environment, cybersecurity has become an essential field because people and organizational information are exposed to additional cybersecurity threats. Artificial Intelligence (AI), in fact, has made a complete revolution in many fields and is also a tool for cybersecurity. Rise of smart surveillance technologies like facial recognition and biometric authentication has been well driven by AI which has heavily propelled abilities for identity verification and security enforcement. However, this overlap with cybersecurity and AI also exposes numerous key legal and ethical issues — related to personal privacy and the preservation of personal identity. [743] As Indian jurisprudence deals with these technological advancements, it must weigh privacy protection against the individual rights of individuals, and privacy in an era of high-tech surveillance and spending adequate, but also adequate, cybersecurity measures. Digital Personal Data Protection Act, 2023, (inspired as personal data protection bill 2019) was aimed at the same issues and therefore help us understand how intricately the AI driven cybersecurity works and the efforts doing India trying to take care of risks and benefits, while trying to achieve the same.

Definition and Scope of Cybersecurity

Defining cybersecurity as the practice of protecting systems, networks, and data from cyber-attack, theft, and damage. Its scope is data protection, network security, application security, information security management, etc. In the legal context, Indian law offers multiple statutory safeguards to enforce cybersecurity from statutory point of view with major frameworks such as "Information Technology Act, 2000" which governs cyber activities and prescribe penalties for the cyber-crimes. With respect to this act 'Section 43' comprises

[743] Matt Hervey and Dr. Matthew Lavy, *The Law of Artificial Intelligence* 105 (Sweet & Maxwell, 2nd edn., 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

unlawful entry while 'Section 66' designs punishments for blockade. Over the last few years, cybersecurity has evolved to accommodate the AI technologies running on massive datasets, including personal information. But these advancements show that cybersecurity laws need to evolve, as cyber threats become more and more sophisticated, and stringent regulations are necessary to protect identity and privacy from malicious AI applications. [744],

Role of AI in Cybersecurity: An Overview

In advancing cybersecurity, AI use machine learning, deep learning, and natural language processing to predict and deal with cyber threats in real time. The primary role of the data science and cybersecurity is to be used for the improvement of the threat detection, risk assessment and response capabilities. Anomaly detection systems based on AI powered solution like AI powered cybersecurity can analyze the traffic pattern in network systems, detect unusual activities, and predict potential cyber-attacks with uncommon accuracies. Across sectors, including banking and healthcare, AI based cybersecurity apps are extensively being adopted in India to secure sensitive data. For example, the AI can reduce the time and resources that require manual cybersecurity monitoring by automating those monotonous tasks. Nevertheless, when AI becomes a part of cybersecurity, legal issues tend to arise, e.g., how to account for AI generated decisions. The application of AI in cybersecurity mandates a robust legal framework that holds organizations accountable for AI-driven cybersecurity measures, as exemplified by cases like *"Shreya Singhal v. Union of India"*[745], which examined the liability associated with intermediary platforms and laid groundwork for future AI-related legal interpretations.

Key Technologies in Smart Surveillance

Smart surveillance technologies like facial recognition, biometric authentication and behavioral analysis are fast becoming fundamental components of the cybersecurity framework worldwide, including in India. Facial recognition, for instance, is already everywhere in identity verification in the banking and law enforcement industry, where biometric authentication now has become commonplace for personal devices and corporate security systems. AI algorithms that enable these technologies are proliferating and can quickly recognize and verify people, making unauthorized access and fraud a thing of the past. Smart surveillance is, however, highly privacy concerned. Facial recognition in public surveillance in India has sparked debate about individual rights under what is called "Article 21 of the Indian Constitution", which aims to give right to privacy as articulated in *"Justice K.S. Puttaswamy v. Union of India"*[746] Such an effort was made in this case, which recognized that privacy is, first and foremost, a fundamental right, restricting the government's surveillance, demanding that infringement of privacy be in terms of legal necessity and proportionality. Therefore, the reliance on AI – driven smart surveillance needs clear statutory regulations to shield people from any possible overreach by public or private entities. [747]

Interplay between AI, Cybersecurity, and Surveillance

The relationship between AI, cybersecurity and surveillance have a dynamic, but difficult relationship to negotiate when it comes to the legal protection of identity and privacy. On the one hand, AI improves cybersecurity by allowing it to survey and detect threats in real time, but on the other hand, it also drives systems of surveillance that could impinge on individuals' rights. Take for instance, advanced AI algorithms, which database their biometric and

[744] Rushil Chandra and Karun Sanjaya, *Artificial Intelligence and Law* 180 (Academic Guru Publishing House, 1st edn., 2024).

[745] (2015) 5 SCC 1.

[746] (2017) 10 SCC 1.

[747] Harry Borovick, *AI and the Law: A Practical Guide to Using Artificial Intelligence Safely* 132 (Apress, Berkeley, CA, 1st edn., 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

behavioral analytics together, to create full profile of the individual, which if misused can lead to identity manipulation, which can be the situation of unauthorized surveillance. With AI in surveillance, Indian legislators are looking at new legal frameworks to ensure the protection of the individuals' autonomy alongside that of national security. The Digital Personal Data Protection Act, 2023 which regulates data collection and processing that collect the biometric data of an individual and use processes it for verification through an electronic device, requires express, prior consent from the individual to these processes protecting personal identities in the field of cybersecurity. "Section 69 of the Information Technology Act" permits government agencies to stitch together digital information for security reasons, but stringent legal procedures are built into it to preclude arbitrary surveillance. Indeed, India's balancing act in the era of AI and evermore intrusive cybersecurity and surveillance rings with dedication to protecting identity. With the evolution of technology, Indian legal frameworks should catch up and the opportunity should be well explored considering the benefits that AI provides, and the risks pertaining to personal privacy and identity should be managed.

LEGAL FRAMEWORK FOR CYBERSECURITY IN INDIA

As the nature of cyber threats in India changes and as more and more aspects of everyday life in India become digitized, India's legal framework for cybersecurity has evolved on the one hand in a slow and gradual manner, and on the other hand through a scattering of recent developments. This Information Technology Act, 2000 is the central framework on which this framework is based and regulates electronic commerce and cybercrimes in India. Since its enactment the IT Act has been amended to the changing cybersecurity worries and moreover gives the legitimate premise for battling the cyber crime, shielding the touchy data and being Sapient. Cyber offenses of data theft and unauthorized access are also under the provision of the Act for which the punishments highlight India's commitment for securing digital space. Besides, the 'Digital Personal Data Protection Act, 2023' (DPDPA) contain provisions for the regulation of protection of personal data and India will conform to international standards about data privacy. Together, it is an attempt to make a whole of the environment approach to better cybersecurity but together starts the need of constant adaptation as technology evolves [748]

Information Technology Act, 2000 and Relevant Amendments

India's principal legislation on cybersecurity is the "Information Technology Act, 2000" under which there are violations relating to unauthorized access, hacking and data theft. Unauthorized access and data damage is repelled by 'Section 43' and 'Section 66' penalizes hacking and carries fines and Imprisonment of perpetrators. Most notably significant about 2008 amendment to the IT Act was the introduction of 'Section 66A' to criminalize offensive online content., though it was later struck down by the Supreme Court in *"Shreya Singhal v. Union of India"*[749] for infringing free speech rights. Such other amendments empowered platforms to sanction a third party for posting content or introduced intermediary liability provision under 'Section 79' under which platforms became liable for third party content. The rise of AI complicates enforcement, bringing this framework to the fore the need for intermediaries to exercise due diligence. AI powered systems on platforms have the potential to inadvertently lead to privacy breaches for which we can't hold companies accountable.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is an important milestone in creating India's robust data privacy framework. This Act is

[748] Giovanni Casini, Livio Robaldo, and Leendert van der Torre, *Handbook of Legal AI* 220 (College Publications, Paperback, 1st edn., 2022).
[749] (2015) 5 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

particularly relevant in the context of Artificial Intelligence (AI) because it is focused on data processing with the individual's consent and outlines severe consequences for data breaches. As a case in point, "Section 11" of the DPDPA permits entities to collect or keep an individual's biometric data only with consent and for specific purposes, including running AI – driven surveillance. It is also important, because it aims to find a fair balance between offering the security benefits AI can provide, on the one hand, and protecting personal privacy, on the other. Moreover, the Act stipulates that data should be collected and processed to the lowest degree possible in order to ensure a further protection of individual privacy. The DPDPA reflects that data usage is managed with risk in mind, and even more so where AI and automation are concerned. However, enforcing the DPDPA in highly automated environments presents challenges: the challenge of a truly informed consent is getting trickier as AI algorithms get more complex. However, the DPDPA is nonetheless a dramatic improvement to the architecture of India's cybersecurity regime, by incorporating transparency and accountability to data processing. However, the Act will need to be periodically reviewed and further refined if it is to retain relevance in the face of a very fast moving evolution in AI and related technologies to remain effective. [750]

National Cyber Security Policy, 2013 and Proposed Updates

India's first attempt at creating a comprehensive cybersecurity policy, "National Cyber Security Policy, 2013" aimed at securing critical information infrastructure and a secure cyberspace. The policy seeks to ensure confidentiality, integrity and availability (an aspect of availability) of digital assets, thus signaling India's preparedness to meet cyber challenge. Given that AI continues to play an ever more central role in cybersecurity, there are arguments for reforming this policy to incorporate potential AI risks and for a more rigorous set of identity protection rules in surveillance. Among proposed updates to the National Cyber Security Policy are plans for building AI capabilities designed to predict and mitigate cyber threats. In 2013 AI was beginning to enter as an emerging standard and the new policy was recognizing the need for skilled cybersecurity professionals which has only intensified since. But as national security in particular brings AI equippers like facial recognition online, innovation in policy is needed to ensure that the risk to individual privacy is not made worse. The emphasis is on strengthening cybersecurity, and at the same time, promoting technology innovation with the two objectives of keeping the nation safe and private. [751]

Role of CERT-IN and Other Regulatory Authorities

India's cybersecurity framework is facilitated by the Indian Computer Emergency Response Team (CERT-IN — National incident response and monitoring agency). As provided in 'Section 70B of the Information Technology Act", CERT-IN encompasses the nodal point of action for coordinated cybersecurity incident management with immediate response to cyber threat. In the face of the emergence of AI based cyber threats, CERT-IN's scope includes responding to vulnerabilities within AI based systems, which demand special knowledge with respect to rapid response protocols. The second approach might be to make policy and regulatory enforcement a collective effort, in which other regulatory bodies, such as the Ministry of Electronics and Information Technology (MeitY), were involved. The implementation of cybersecurity laws is supervised by MeitY in coordination with CERTIN. Further, the Reserve Bank of India (RBI) has, in particular its cybersecurity guidelines for financial institutions, acknowledged the risk of

[750] Ina Nikolova, "How to Protect Digital Identities in The Era Of AI?", *available at:* https://www.linkedin.com/pulse/how-protect-digital-identities-era-ai-ina-nikolova-ph-d--642af/ (last visited on October 15, 2024).

[751] Sri Yash Tadimalla and Mary Lou Maher, "AI and Identity", 4 *AAAI Spring Symposium* 72 (2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

cyber threats against the sector. In turn, these regulatory bodies work together to enforce cybersecurity standards, although the pace at which the future of AI is developing leaves much to be desired and underscoring the need for a coordinated effort in managing AI risks and the principles of identity protection.

IDENTITY PROTECTION IN THE DIGITAL ERA

Digital identity is the collection and set of information and data points that uniquely identify an individual in an online or electronic context. The identity is made up of many different types of personal data; names, social security numbers, biometric data and the digital footprints individuals leave online in the course of carrying out everyday activities. As we enter the digital age where most of our interactions are digital, this digital identity has been participating as an important part of our personal and professional dealings. From online banking and e commerce transactions to accessing government services or real time identity verification, digital identity makes it all happen. That is why it is such a prime target for malicious actors. In India, where digitalization is being taken up fast, the government has enacted Digital Identity protection Laws among others being the "Aadhaar Act, 2016" for Biometric and demographic information of individuals. With AI surveillance technologies becoming more sophisticated, however, securing and verifying digital identities get more difficult. Digital identity is of utmost importance because any compromise of digital identity can result in different forms of identity theft, financial loss and potential exposure of privacy. [752],

Vulnerabilities in Identity Protection within AI Surveillance Systems

While robust security solutions, AI powered surveillance systems bring in vulnerabilities that can jeopardize identity protection. Biometric data (facial recognition or fingerprint scanning) is often used by these systems, and their breach can reveal individuals to greater odds of harm. While these systems feature one major vulnerability: storing and processing sensitive data, which makes them prone to cyber-attacks. In *"Justice K.S. Puttaswamy v. Union of India"*[753], the Supreme Court of India stressed on right to privacy and ruled, the need for stringent data protection laws, while handling such sensitive personal data as biometrics. But the introduction of AI into surveillance intensifies these worries since AI systems are intended to collect, work and interpret huge amounts of data. The constant data accumulation adds to the risk of unauthorized access which presents a great deal of challenges to protecting identities. Lack of adequate security of surveillance systems may unintentionally reveal the biometric and other personal data, which in turn are a threat to digital identity. With surveillance incorporating more of AI, digital identity security remains at the top of lawmakers' and cybersecurity experts' minds.

Threats Posed by Data Breaches and Identity Theft

Two of the biggest threats to digital identity in today's digital world are data breaches and identity theft. A data breach happens when bad people get access to data that they're not supposed to have access to, and sometimes that data contains somebody's personal information and can be used to do bad things, like commit identity theft. Identity theft is another term for when a person's personal data is stolen and fraudulently used, usually for financial advantage or for the purpose of committing more crimes. The 'Digital Personal Data Protection Act, 2023' ('DPDPA') makes its debut in India, attempting to protect personal data and address these dangers by imposing stringent demands on entities that possess sensitive data ensuring these data are secure. The Act requires organizations that collect and process personal data to secure it properly, and must gain explicit consent from the individual.

[752] Milad Mirbabaie, Felix Brünker, et. el., "The Rise of Artificial Intelligence: Understanding the AI Identity Threat at the Workplace", 32 *Electronic Markets* 55 (2021).

[753] (2017) 10 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

However, the risk is further compounded by AI driven surveillance systems that continually collect and store vast amounts of data. The integration of AI into so many public and private surveillance platforms indicates that AI may somehow significantly increase the ability to identify and track people by simply matching their face, pose and gesture. Data protection and breach prevention are fundamental aspects of cybersecurity law because identity theft results in serious consequences that extend far beyond the loss of finances, negatively impacting an individual's credit score and intimate relationships, as well as their overall quality of life. [754]

Role of AI in Both Protecting and Compromising Identity

In the land of identity protection, AI wears two hats; it can protect and it can also compromise digital identity. On the other hand, AI powered systems can improve identity verification by using more sophisticated algorithms which detect anomalies in digital interactions, identifying possible identity theft raids. For example, biometric authentication systems, powered by AI, can very effectively and efficiently verify identities based upon unique biological traits that are more difficult to replicate than the use of traditional passwords. On the other hand, though, these same AI technologies also put identity at risk due to the data they need to collect, and the sensitive information they store. In fact, an AI facial recognition system, for instance, could easily be hacked, leading to many biometric data exposed, that makes individuals vulnerable to identity theft.

CHALLENGES IN SAFEGUARDING IDENTITY WITH AI AND SURVEILLANCE

In recent times, with the advancing age of AI Barak in surveillance, there has been a rising debate in legislation and the broader society around which issues should privacy and security be balanced. Surveillance systems are critical in increasing security in populous nations such as India, they, however, counterweigh on individual privacy rights. Facial recognition, behavioral analysis, and biometric identification technologies driven by AI are being deployed even more widely now to prevent crime and to better protect public safety and security. The problem is that these tools collect too much personal information which can, ultimately, infringe on certain individuals' privacy rights guaranteed under "Article 21 of the Indian Constitution." The Supreme Court of India, in *"Justice K.S. Puttaswamy v. Union of India"*[755], recognized the right to privacy as a fundamental right, it also laid down the constitutional basis for holding the balance between security and freedom of individual. But while AI surveillance continues to become ever more pervasive, it carries ever greater risk to civil freedoms. Thus, lawmakers must reach a careful but delicate balance between maximum security and the intrinsic right of privacy for citizens.[756]

Legal and Ethical Challenges in AI-Powered Surveillance

There are also many serious legal and ethical issues with deploying AI powered surveillance systems. One thing AI is good for is processing lots of data fast and this ability makes it a thing that can help us monitor public areas and predict crime patters. But AI in surveillance can be misused and rights can be violated without adequate legal safeguards, data abused and the fault unaccounted for. Take, for instance, predictive policing technologies which leverage AI to forecast crime hotspots and thereby unknowingly generate ethical dilemmas via increased racial profiling and discrimination of the AI used in law enforcement. In India there is no specific laws to monitor the AI surveillance

[754] Katharine Miller, "Privacy in an AI Era: How Do We Protect Our Personal Information?", *available at:* https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information (last visited on October 16, 2024).

[755] (2017) 10 SCC 1.

[756] Deepak Gupta, "The AI Paradox in Digital Identity: Why More Security Might Mean Less Privacy (And What to Do About It)", *available at:* https://guptadeepak.com/the-ai-paradox-in-digital-identity-why-more-security-might-mean-less-privacy-and-what-to-do-about-it/ (last visited on October 17, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

and there is lot of ambiguity, which means an accountability window is missed. The only existing legal provisions on AI driven surveillance that do exist in India are the "Information Technology Act, 2000" and the most recent "Digital Personal Data Protection Act, 2023", but these are rather scant on guidelines. Therefore, ethical principles like transparency, accountability, fairness, must be weaved into AI surveillance technologies to protect against misuse, and operate within legal and moral confines.

Issues of Consent, Autonomy, and Data Misuse

AI surveillance lacks informed consent which lowers individual autonomy being the central issue with it. More generally public space AI surveillance systems are collecting data on people who are typically not aware of that, and don't give their consent to that. And in turn this creates very serious questions about what is at the core of personal autonomy in terms of control over the collection, storage and use of personal data. Among them was the prohibition of data collectors to process personal data without the explicit consent of the person who is concerned with processing. However, when it comes to AI surveillance, informed consent is practically impossible to come by, much of this because AI surveillance systems are routinely installed without anyone's knowledge. But there's worse: As AI systems can be hacked, accessed by unauthorized parties for using the data in case required. Therefore, instances of data misuse can be relied upon to identify the basis of identity theft, financial loss and even emotional distress, thus emphasizing the need for strict regulations to prevent predators from getting hold of data. As a consequence within a digitally developed society, consent and transparency in the use of AI are therefore critical if these individual rights are to be respected by AI surveillance systems. [757],

Case Studies on AI and Identity-Related Security Breaches in India

Some instances from India show how AI and surveillance technologies deal with identity security risks. That brings us to one particularly prominent case of such a breach, that of the Aadhaar database—a database of biometric and demographic data on millions of Indian citizens. In 2018, a report claimed that one could get access to Aadhaar data through unofficial channels at small remuneration which raises security doubts of people data stored in various government databases. The Aadhaar breach illustrates how data protection system vulnerability, with special reference to AI enabled biometric verification system, leads to identity theft and allow unauthorized access. Views have also come in that the incident highlighted why India needs to have tight cybersecurity measures in place and that there needs to be a robust data protection framework that needs to be adopted by the Indian government. The public was also made unaware that data was being collected when facial recognition technology was used at public events. These cases remind us that there is an imperative to have adequate legal safeguards in place to ensure that AI and surveillance technology are used responsibly, and in accordance with the rights of persons and data protection. As AI surveillance marches ahead, India's legal framework must ensure that these capabilities remain contained within the framework so our citizens are not at risk of being quite possibly privatized and identity related creeps.[758]

INTERNATIONAL COMPARISON

Cybersecurity and AI identity protection standards globally are diverse with leading frameworks emphasizing the protection of personal data and setting tough limits for data collection as well as processing. General Data Protection Regulation (GDPR in the European

[757] AI-Powered Behavioral Analysis for Identity Security, *available at:* https://www.kiwitech.com/blog/ai-powered-behavioral-analysis-for-identity-security/ (last visited on October 18, 2024).

[758] Sanjay Vaid, "Impact Assessment of Artificial Intelligence on Cybersecurity: A Review of the Existing Literature", 25 *FOCUS WTO* 13 (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Union) sets a global example when it comes to privacy laws and includes regulatory rules for data controllers and processors. Under the GDPR, data aggregation for AI surveillance technologies requires explicit consent, as well as to be subject to particular stringent data processing standards. The United States shares this similarity, as though federal data protection laws are fairly restrictive, industries such as healthcare, consumer services, etc. have sector specific regulations (HIPAA, CCPA) that require identity protection and data security. For its part, China chooses a more government – oriented solution with its Cybersecurity Law and Personal Information Protection Law (PIPL) favoring the national security by massive surveillance and data control inside the national fabric. These frameworks reflect the different regulatory philosophies, ranging from individual rights in the EU, sectoral autonomy in the U.S. and state control in China, and demonstrate a variety of global standards in controlling AI powered cybersecurity for identity protection.[759]

Case Studies from the USA, EU (GDPR), and China

Using case studies of the United States, the European Union, and China, I show how these regions build upon their individual regulatory frameworks to protect personal identity and manage AI-based surveillance. The 2018 Facebook-Cambridge Analytica scandal showed how AI driven algorithms were exploiting user data without consent in the U.S. Such was the case also in this case, where it demonstrated the need for better federal regulation to guard individual's personal information from irresponsible commercial misuse, followed by a more careful look into this data handling practice in the technology sector. However, the European Union's GDPR is an example of proactively applied legal oversight. In 2019, Google was slapped with a large fine under the GDPR for lack of transparency in data processing — all illustrating the EU's dedication to individual privacy rights. China's case studies are distinctive chiefly because the AI surveillance technologies are embedded in its social credit system, a system which ranks citizens by their behavior. While controversial, this model reflects China's way of forging through extensive state surveillance to maintain law and order, provoking ethical and privacy questions. Vying regulatory responses to comparable difficulties demonstrate different ranges of regulative advancement's adjustability versus the requirement for identification protection.[760]

Comparative Analysis: India's Position on the Global Stage

India's approach to cybersecurity and AI driven-identity protection is developing in comparison with these global frameworks and is a mix of legislation and regulatory challenges. India's 'Digital Personal Data Protection Act, 2023' (DPDPA) though, like the GDPR, focusses on consent and data minimization, it lacks the GDPR's enforcement mechanisms and comprehensive infrastructure. India also lags because it continues to use the harmful model of the 'Information Technology Act, 2000' and its amendments, which do not deal with AI issues completely. The fact remains, however, the DPDPA is a major move forward in laying the foundations of identity protection, embedding penalties for non-compliance, and introducing explicit and clear agreements on consent. Where India's regulatory landscape is favored compared to China's, privacy versus state surveillance takes the stronger position and corresponds to what can be considered Western ideas about autonomy of the individual, as protected by *"Justice K.S. Puttaswamy v. Union of India"*[761]. Even though India is making ambitious digitalization efforts, it

[759] Artificial Intelligence v/s Cyber Security: Which career is better?, *available at:* https://www.edology.com/blog/artificial-intelligence-and-machine-learning/artificial-intelligence-vs-cyber-security_which-career-is-better/ (last visited on October 15, 2024).

[760] Nick Wallace and Daniel Castro, The Impact of the EU's New Data Protection Regulation on AI, *available at:* https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf (last visited on October 15, 2024).

[761] (2017) 10 SCC 1.

still has challenges in implementation, enforcement. But in looking to see India become a global technology leader, a stronger AI specific regulatory framework is essential to protect identity while encouraging technological growth so that the country continues to remain competitive in the world arena.

ROLE OF AI IN STRENGTHENING CYBERSECURITY LAWS IN INDIA

Transformative, Artificial Intelligence (AI) may contribute to bolstering cybersecurity laws in India by helping to detect and prevent cyber threat. Machine learning algorithms are used in AI driven tools to analyze significant amounts of data to discover patterns, and predict cyber-attacks before they take place. AI can identify possible threats in real time by utilizing techniques such as anomaly detections within the system itself. Such predictive capabilities are critical in India where digitalization has been rapidly expanding and sensitive data and national security needs protecting. For instance, AI is able to spot phishing attempts by looking at features of email structure and sender behavior, and alerting about threats faster than traditional cybersecurity systems. Automation further supports this proactive approach by allowing AI to do the repetitive security tasks well, and only raise an alarm to human operators in high-risk situations. High rate of cyber threats in India means that AI has crucial role in detecting and preventing attacks, much in sync to the legislative efforts to strengthen India's cybersecurity and protect individual identities.[762]

Smart Surveillance vs. Smart Protection: Ethical Implications

The use of smart surveillance for identity protection in cybersecurity is an ethical question with a subtle aspect when AI is added to the mix. Even though AI powered surveillance system enhances security by scouting and recognizing possible dangers, they become a reason of concern as while they quench security, they take away privacy and individual autonomy. The Indian Constitution, in *"Justice K.S. Puttaswamy v. Union of India"*[763], The right to privacy is enshrined and any invasion must be proportionate, and in the interests of the public. This precedent puts a moral burden on AI surveillance to play by the rules of freedom which should be applied to people. AI tools, as such, inherently collect massive amounts of data which can be misused, unless regulated, and balancing security needs against civil liberties is complex. Taking cybersecurity first depends on smart surveillance, but it must live side by side with smart protection rules that preserve privacy and guarantee proper treatment of data. An Indian cybersecurity framework, therefore, will only progress if these AI applications are designed with built in safeguards respecting human rights that together build a security system that enables both protection and privacy.

Current AI Solutions in Cybersecurity by Government and Private Sectors

More and more government and private sectors in India are using AI solutions for cybersecurity, understanding that AI is an important solution to sophisticated cyber threats. In parallel, the Indian government has launched a series of initiatives, with the Centre for Development of Advanced Computing (C-DAC) developing AI driven solutions to strengthen the infrastructure of cybersecurity. Even the Indian Computer Emergency Response Team (CERT-IN) is at the helm of hype, which, in collaboration with AI technologies, scans through cyber threats and vulnerabilities, and provides incident response mechanisms to protect critical infrastructure. In the private sector, AI vendors such as Tata Consultancy Services (TCS) and Wipro are building out security frameworks for real time threat detection and response. Tools that would only scan networks for irregular activities and

[762] Aditya Narayan Choubey, "Strengthening National Cybersecurity of India with the Use of Artificial Intelligence", *available at:* https://cenjows.in/strengthening-national-cybersecurity-of-india-with-the-use-of-artificial-intelligence/ (last visited on October 15, 2024).

[763] (2017) 10 SCC 1.

give proactive insights into risks are utilized by these companies. Although these solutions hold promise, they need regulatory guidance to integrate AI into cyber security, avoiding rights violation of privacy or excessive surveillance. The government-private sector collaboration promises a future where India's cyberspace will be properly secured, and the contribution made by the emergence of AI warrants the making of AI-specific cybersecurity laws to responsibly guide these applications.

Emerging AI-Powered Strategies for Identity Protection in India

One of India's saving graces in the world of cybersecurity is the emerging AI powered identity protection strategies – they increasingly rely on biometric verification and multi factor authentication systems. Facial recognition and fingerprint scanning biometric tools, allow greater security for identity verification as it is more difficult for unauthorized individuals to view sensitive information. The use of such biometric data does bring with it problems around storage and privacy however, with processing giant amounts of personal data. Behavioral biometrics are also an AI driven identity protection strategy whereby the AI analyses the pattern of typing speed, swipe gestures and user interaction, in conjunction with other factors, to authenticate identity. Traditional passwords are vulnerable to theft and hacking so this method of passive authentication reduces such dependence. The "Digital Personal Data Protection Act, 2023" makes consent a pre requisite of any sort of collection of personal data, including biometric and behavioral data, to be utilized ethically as well securely. With AI in the mix, India's cybersecurity is taken to the next level, and it's time for regulations that will allow these tools to operate within a secure, ethical context. The strategies that India adopts in response to this growing threat must continue to evolve, so as to realize AI's potential in the realm of protecting identity while protecting the rights of the citizen to their privacy and the security of their data.[764]

CONCLUSION

The integration of Artificial intelligence (AI) in cybersecurity and surveillance holds a prominent landmark of safeguarding the digital identity which is leaping in India's growing digital ecosystem. AI (Artificial Intelligence) powered surveillance systems offer a great potential in offering security through real time monitoring, threat detection, and identity verification can be possible. Yet, the abundance of personal data gathered by surveillance technologies threatens privacy and identity protection while evoking legal, ethical, and regulatory problems. As this research reveals, India has indeed advanced in legislating these laws, including the "Information Technology Act, 2000" and the recently passed "Digital Personal Data Protection Act, 2023" (DPDPA), but these frameworks need to be fine-tuned to appropriately cover the requirements of AI driven cybersecurity and surveillance.

The IT Act based framework for cybersecurity in India is focused on penalties for cybercrimes and on data protection. The DPDPA is a new approach to data protection which focuses on consenting personal data collection and puts accountability back on organizations that control sensitive information. But these regulations have limitations that do not fully meet AI's effects, especially with surveillance systems in which lines between security and privacy become blurred. The judiciary, as evidenced in cases like *Justice K.S. Puttaswamy v. Union of India*[765], privacy is being underscored as a basic right, the implementation of privacy in AI assisted surveillance is practically challenging. India's current laws should be modified to incorporate the specificities of protecting identity in AI-related issues, as both one's dynamic consent and the consequences that derive from its use of biometric data.

[764] S Prabhakar, I Nalinaksha, and V Anjaneyulu, "Role of AI in enhancing cybersecurity measures to protect sensitive financial data", 10 *International Journal of Science and Research Archive* 1091 (2023).
[765] (2017) 10 SCC 1.

The European Union's General Data Protection Regulation (GDPR) and sector specific regulation in places like the United States serve as the gold standard of privacy and data security regulation globally. While India's DPDPA shares many similarities to GDPR principles, there are no stringent enforcement mechanisms, and usage of AI in relation to DPDPA is ill defined. Comparing to China, a contrasting regulatory philosophy priority on the surveillance in the hand of state control. Although India lines up with the EU on the privacy front, it needs to strengthen its enforcement capabilities and gear up for quickly evolving AI regimes to stay competitive internationally.

AI plays a dual role of protecter and possible violator of identity that require a balanced legal regime to reap the benefits of AI while avoiding the risks. Transparency, accountability and ethical AI deployment must be featured in legal reforms. For example, safeguards must be in place for AI powered smart surveillance systems--in the event that the data is used illegally and breached. Furthermore, ways of integrating consent mechanisms into AI systems could enforce individual autonomy even over publicly deployable surveillance technologies. Additionally, tighter data protection measures should follow alongside the progressive technology of AI in identity protection including biometric and behavioral authentication, to prevent the misuse of sensitive data.

The roles that AI driven cybersecurity threats have to be addressed by India's regulatory authorities, namely CERT, IN and Ministry of Electronics and Information Technology. While emerging cybersecurity risks need to be mitigated, coordination among the agencies remains effective, AI specific guidelines need to be enhanced, and collaboration with the private sector is needed.

Finally, AI offers India unprecedented capability in cybersecurity and surveillance but potentially subverts India's legal framework for identity and privacy in a world becoming rapidly digitized. India can protect its own citizens' identities, and those of other countries, from AI driven risks, responsibly, by evolving its own laws to manage them. Future legal reforms in India should deal with the technical aspects of AI as well as appropriate protections for individual's rights, in order to ensure that India's cybersecurity laws do not remain behind the complexities of digital age. And we will continue all the holiday shopping while hacking away at dragons.

SUGGESTIONS

To address the complexities of identity protection within AI-driven cybersecurity and surveillance in India, it is crucial to implement targeted, actionable reforms within existing legal frameworks:

1. Establish clear guidelines on data minimization for AI-based surveillance systems to prevent excessive data collection. This will help ensure that only essential data is processed, reducing the risk of unauthorized access and identity breaches.
2. Strengthen enforcement mechanisms in the "Digital Personal Data Protection Act, 2023" to include specific penalties for misuse of AI in surveillance. This would hold organizations accountable for breaches and promote responsible data handling practices.
3. Introduce mandatory transparency requirements for organizations deploying AI surveillance tools, such as periodic reports on data collection and processing activities. This can enhance public trust by allowing individuals to understand how their data is used and safeguarded.
4. Develop a centralized regulatory body to oversee AI applications in cybersecurity and surveillance, coordinating efforts between agencies like CERT-IN and MeitY. A unified approach can streamline

policy enforcement and reduce regulatory ambiguities.

5. Incorporate international best practices, such as GDPR-aligned consent mechanisms and data portability rights, to strengthen Indian laws. This adaptation will ensure India's cybersecurity framework remains globally competitive while protecting individual privacy rights.