Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Fingerprints, Iris Scans, and the Law: Regulating Biometric Human-Computer Interfaces

Shikhar Srivastava[1], Diwakar Harit[2], Abhishek Panwar[3]
[1]*Assistant Professor*
School of Law, JECRC University, Jaipur, Rajasthan
Email Id: shikhar.icai@gmail.com
Mobile No.: 9311407212
[2]*Assistant Professor*
School of Law, JECRC University, Jaipur, Rajasthan
Email Id: diwakarharit@gmail.com
Mobile No.:8005548807
[3]*Assistant Professor*
School of Law, JECRC University, Jaipur, Rajasthan
Email Id: abhishekpanwar41@gmail.com
Mobile No.: 8394088850

ARTICLE INFO

Received: 20 Oct 2024

Revised: 22 Nov 2024

Accepted: 24 Dec 2024

ABSTRACT

Household budgeting is crucial for financial stability, yet many individuals find it challenging due to the lack of structured financial planning tools. This paper introduces a rule-based system that optimizes expenses by considering family size, age distribution, income, and overall budget. Unlike traditional budgeting tools, our system dynamically distributes income across essential categories—such as housing, food, medical care, education, and savings—using predefined rules. The system leverages dynamic input processing and rule-based allocation to provide real-time insights into budgeting constraints. Upon completing the expense distribution, the system evaluates whether the household maintains a cash in hand or requires debt payment, offering actionable financial insights. Experimental results show that the proposed model achieves 90% accuracy in budget allocation, ensuring financial sustainability and preventing overspending. The system offers a transparent, flexible, and user-friendly alternative to machine learning-based budget models, making it accessible to households of all financial backgrounds.

Keywords: Household budget, income tracking, rule-based system, financial management, expense monitoring.

Introduction

In an era where technology mediates nearly all aspects of human life, biometric human-computer interfaces (HCIs) have emerged as powerful tools for identification and access control. From unlocking smartphones using fingerprints to scanning irises for access to public welfare systems, biometric data is now integral to how individuals interact with machines. However, this increased reliance on biometrics brings with it complex legal and ethical concerns, particularly around user privacy, informed consent, data storage, and the potential for surveillance. The law must grapple with how to regulate these interfaces in ways that preserve individual rights while accommodating technological innovation. This paper investigates these concerns by analyzing the legal frameworks that govern biometric interfaces, particularly in India, while drawing comparisons with international regimes such as the European Union's GDPR and the United States' BIPA.

Biometric human-computer interfaces (HCI) refer to systems and technologies that enable interaction between humans and computers using unique biological or physiological traits for identification, authentication, or access control. These interfaces capture and process individual biometric data—such as fingerprints, iris patterns, facial features, voiceprints, or even gait and heartbeat rhythms—to allow seamless, secure, and often touchless communication between a user and a machine.

Biometric HCIs are increasingly integrated into everyday technologies, including smartphones, ATMs, border security systems, workplace access controls, and digital identity platforms. Unlike traditional authentication methods

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

like passwords or PINs, biometric interfaces rely on inherent user characteristics, making them more personal, but also raising complex legal, ethical, and privacy concerns, especially related to consent, data protection, and potential surveillance.

Biometric human-computer interfaces have become deeply embedded in modern technology, transforming the way individuals interact with digital systems. In consumer electronics, smartphones now routinely use fingerprint sensors and facial recognition for device unlocking and mobile payments, offering users both convenience and enhanced security. In enterprise and security environments, biometric access control systems manage entry to sensitive locations through iris scans or fingerprint verification. Public services too have adopted biometric interfaces at scale—most notably in India through the Aadhaar system, which uses fingerprints and iris scans to authenticate identity for millions of citizens accessing government benefits and financial services. As these technologies become more prevalent, they not only increase efficiency and security but also raise pressing legal and ethical questions about surveillance, data misuse, and individual autonomy.

While biometric interfaces offer clear advantages in terms of security and user convenience, they simultaneously introduce complex legal dilemmas that are yet to be fully addressed. On one hand, the use of fingerprints or iris scans can drastically reduce identity fraud, streamline verification, and personalize user experiences. On the other hand, these same features pose significant threats to privacy when biometric data is collected without informed consent, stored insecurely, or repurposed beyond its original use—a phenomenon known as function creep. Unlike passwords, biometric data is immutable; once compromised, it cannot be changed. This makes the consequences of data breaches far more severe. Furthermore, the widespread deployment of biometric systems by both state and private actors raises concerns of mass surveillance and erosion of civil liberties, especially in the absence of robust legal safeguards. This tension between technological advancement and the protection of fundamental rights underscores the urgent need for a clear, comprehensive legal framework governing biometric human-computer interaction.

Research Objectives and Questions

The objective of this research is to critically examine the legal challenges and regulatory frameworks surrounding the use of biometric human-computer interfaces (HCIs), with a focus on fingerprint and iris scan technologies. The paper aims to explore how biometric data is collected, processed, and protected in digital systems, particularly in the context of India's legal landscape, while drawing comparisons with international standards. It seeks to evaluate the adequacy of existing laws in safeguarding individual rights, highlight gaps in policy, and propose recommendations for responsible and privacy-compliant biometric regulation.

Key Research Questions:

1. What legal frameworks currently govern the use of biometric data in human-computer interfaces in India and internationally?
2. To what extent do these laws ensure user consent, data security, and protection against misuse or surveillance?
3. What are the legal and ethical risks associated with the use of biometric HCIs, particularly in public services and private sector applications?
4. How have courts in India and other jurisdictions interpreted the right to privacy and data protection in the context of biometric technologies?
5. What legal reforms and human-centered design principles can be recommended to ensure that biometric interfaces respect fundamental rights while supporting technological innovation?

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Literature Review

The intersection of biometric technology and law has attracted growing academic attention, especially in the wake of global privacy debates and the expansion of digital identity systems. Scholars have broadly examined biometric systems through lenses of privacy, surveillance, consent, and legal accountability.

Daniel J. Solove (2008) emphasizes that biometric data must be seen as part of the broader architecture of "information privacy," arguing that traditional consent models are insufficient in a digital ecosystem where data can be reused, repurposed, and stored indefinitely. Helen Nissenbaum's *Privacy in Context* (2010) complements this view by stressing the importance of "contextual integrity"—the idea that privacy is breached not merely when data is shared, but when it flows outside its expected context, a common occurrence in biometric systems.

In the Indian context, Rahul Matthan (2021) critiques the Aadhaar system for adopting a techno-centric approach without embedding adequate safeguards for user consent and redressal. Similarly, the Internet Freedom Foundation (IFF) has raised consistent concerns about the risk of mass surveillance and biometric data breaches, especially in the absence of a robust data protection law until the recent enactment of the Digital Personal Data Protection Act (DPDPA), 2023.

On the international front, scholars analyzing the European General Data Protection Regulation (GDPR) point out that it treats biometric data as "special category data," subject to stricter processing rules. Binns and Veale (2018) argue that the GDPR model offers a strong foundation for rights-based regulation but note challenges in operationalizing transparency and algorithmic accountability in biometric interfaces.

In contrast, the U.S. approach has been sectoral and state-specific, with the Illinois Biometric Information Privacy Act (BIPA) serving as a rare example of a strong legal framework. Litigations under BIPA (e.g., *Rosenbach v. Six Flags*) demonstrate an emerging body of case law where courts have recognized individuals' right to sue even in the absence of actual harm, thereby setting a high standard for consent and notice.

This literature reveals a growing consensus on the need for legal reform and stronger user-centric safeguards in biometric regulation. However, gaps remain in addressing **cross-border data transfers**, **private sector responsibilities**, and **the role of HCI design in ensuring legal compliance**—areas this research aims to explore further.

Comparative Legal Framework

The legal treatment of biometric data varies widely across jurisdictions, reflecting different constitutional traditions, levels of technological adoption, and approaches to data protection. This section compares the legal frameworks of **India**, the **European Union (EU)**, and the **United States (US)** in regulating biometric human-computer interfaces.

A. India: A Growing Regulatory Framework with Foundational Challenges

India's approach to biometric regulation has been largely shaped by the Aadhaar system, the world's largest biometric ID program. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 governs the collection of fingerprints and iris scans for identity verification. However, Aadhaar faced intense legal scrutiny in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where the Supreme Court declared privacy a fundamental right under Article 21 of the Constitution. While Aadhaar was upheld as constitutional with limitations, the court emphasized the need for minimal data collection, informed consent, and robust safeguards against surveillance.

The **Digital Personal Data Protection Act, 2023 (DPDPA)** is India's first comprehensive data protection law. It classifies biometric data as "personal data" but stops short of defining it as a special or sensitive category, unlike the GDPR. The law requires that consent be "freely given, specific, informed and unambiguous," but enforcement mechanisms, sectoral guidelines, and data localization rules remain under development. Moreover, there is limited clarity on private sector obligations and biometric data sharing with law enforcement.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

B. European Union: A Rights-Based and Robust Legal Framework

The **General Data Protection Regulation (GDPR)** treats biometric data as a "special category of personal data" under Article 9, thus prohibiting its processing unless specific legal conditions are met—such as explicit consent, public interest, or employment law compliance. The GDPR emphasizes data minimization, purpose limitation, and user rights including access, correction, and erasure.

The **principle of privacy by design and by default** is central to the EU's legal approach, making it legally necessary for HCI systems to incorporate privacy-enhancing measures from the outset. In decisions like *Schrems II*, the Court of Justice of the European Union has demonstrated a strong commitment to individual rights in data transfers, setting a high bar for third-country access to EU residents' data—including biometrics. Importantly, EU regulators have begun issuing fines to companies that collect biometric data without proper legal grounds, reinforcing compliance through financial penalties.

C. United States: Fragmented but Litigation-Driven Protection

The United States lacks a comprehensive federal law on data protection. Instead, biometric data regulation is driven by state laws, the most notable being the **Illinois Biometric Information Privacy Act (BIPA)**. BIPA mandates that private entities must obtain informed written consent before collecting biometric identifiers such as fingerprints, iris scans, or facial geometry. It also requires public notice, data retention schedules, and prohibits the sale of biometric data.

Significant case law, such as *Rosenbach v. Six Flags Entertainment Corp.* (2019), has expanded standing under BIPA, allowing individuals to sue even when no tangible harm can be shown. This has led to a surge in class-action lawsuits against companies like Facebook and TikTok, pushing the private sector toward higher compliance. However, the lack of a uniform national standard creates regulatory uncertainty, especially for companies operating across multiple states.

Key Comparative Observations

Aspect	India	European Union	United States (Illinois)
Legal Framework	Aadhaar Act, DPDPA 2023	GDPR	BIPA (State-level)
Biometric as Sensitive Data?	Not explicitly	Yes (Article 9 GDPR)	Yes
Consent Requirement	Required but loosely defined	Explicit, informed, and documented	Informed written consent
Enforcement Mechanism	Developing	Strong, centralized (EDPB)	Litigation-driven
Design Mandates (HCI)	Lacking	Privacy by Design required	No specific mandates
Private Sector Coverage	Partial	Comprehensive	State-specific

Legal and Ethical Concerns

Biometric human-computer interfaces (HCIs) offer undeniable advantages in terms of convenience, security, and accessibility, but they also introduce a range of legal and ethical concerns. These concerns primarily revolve around the **privacy of individuals**, **data security**, and the **ethical implications of surveillance** and **consent**.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. Consent and Informed Decision-Making

One of the central ethical challenges surrounding biometric HCIs is ensuring that individuals give **informed consent** for the collection and use of their biometric data. The unique nature of biometric data, such as fingerprints and iris scans, means that once compromised, it cannot be changed like a password. This makes consent a critical issue. In practice, obtaining truly informed consent can be difficult, particularly in systems where users may feel pressured to comply (e.g., when biometric data is used for government benefits, or access to essential services like healthcare or banking). The question remains: Can an individual ever freely consent when the stakes of non-compliance are so high?

2. Data Security and Risk of Breaches

The security of biometric data poses significant legal risks. Unlike other forms of personal information, such as usernames and passwords, biometric identifiers are inherently permanent and cannot be changed if exposed in a data breach. The theft or misuse of biometric data, such as fingerprints or iris scans, carries much greater consequences than the loss of a password.

In **India**, the Aadhaar data breach in 2018 exposed millions of biometric records, highlighting the risks of data storage on centralized servers. Although the **Digital Personal Data Protection Act, 2023** introduces provisions for data protection, including penalties for non-compliance, **data security** continues to be a major concern. The potential for biometric data to be misused or sold on the black market underscores the need for stringent legal frameworks to ensure that biometric systems are built with robust **security measures** that comply with evolving standards.

3. Function Creep: From Authentication to Surveillance

Biometric data, originally collected for specific purposes, often gets repurposed in ways that violate the expectations of users—a phenomenon known as **function creep**. Initially collected for security or identity verification, biometric data may later be used for purposes like tracking individuals across public spaces or profiling them for marketing. This raises significant **ethical concerns** about **surveillance** and **civil liberties**.

A notable example of function creep is the **Aadhaar system** in India, which was originally designed for the delivery of public services but has been extended to areas such as voter registration and mobile phone verification. Critics argue that such extensions of biometric data usage risk turning the system into a tool for **mass surveillance**, where the government can track individuals' movements, behaviors, and transactions, potentially violating fundamental rights to privacy and freedom.

4. Bias and Discrimination in Biometric Systems

Another important concern is the potential for **bias** and **discrimination** in biometric technologies. Numerous studies have shown that biometric systems, particularly those relying on facial recognition, can exhibit racial, gender, and age-based biases. For example, facial recognition systems have been shown to be less accurate in identifying people of color and women, leading to the risk of wrongful identification, discrimination, or exclusion from access to services.

In the legal context, the unequal accuracy of these systems may lead to **unintended legal consequences**, such as **wrongful denial of access** to public services, financial systems, or employment opportunities, potentially infringing on the **right to equality**. Legal frameworks must not only regulate the collection and use of biometric data but also mandate that biometric systems are **inclusive, unbiased**, and **fair**.

5. Surveillance and Privacy Violations

The growing use of biometric technologies by both governments and private entities raises the specter of pervasive **surveillance**. With biometric systems, it becomes possible to track and monitor individuals' movements, activities, and interactions without their knowledge or consent. This potential for surveillance poses grave concerns for **privacy** and **autonomy**.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Mass surveillance via biometric systems is already a reality in some jurisdictions, such as China's use of facial recognition for monitoring citizens. In India, the **Aadhaar system** has faced criticism for enabling surveillance-like capabilities, despite legal safeguards in place. In the EU, although the **GDPR** has been a strong step toward protecting privacy, concerns about surveillance through **video surveillance and facial recognition** in public spaces persist. Legal protections must ensure that biometric technologies are not used to infringe on an individual's right to privacy or to engage in covert, undemocratic surveillance.

Regulatory Gaps and Need for Reform

Despite the growing use of biometric human-computer interfaces (HCIs), the legal and regulatory frameworks governing these technologies remain fragmented, incomplete, and often outdated. As biometric systems proliferate, they raise fundamental questions about data protection, privacy, surveillance, and human rights. Existing laws have not fully adapted to the rapid pace of technological advancements, leading to **regulatory gaps** that expose individuals to risks such as **data breaches**, **unauthorized surveillance**, and **discrimination**. This section identifies the critical gaps in current regulations and proposes reforms needed to ensure that biometric systems are legally compliant, ethically sound, and privacy-respecting.

1. Inadequate Legal Definitions and Scope

A primary gap in many legal frameworks, including **India's Aadhaar Act** and the **Digital Personal Data Protection Act (2023)**, is the lack of clarity regarding the **legal definition** of biometric data. While some frameworks treat biometric data as a form of **personal data**, few give it special status as a "sensitive" category, despite its unique vulnerabilities. In comparison, the **GDPR** classifies biometric data as a "special category of personal data," requiring stricter protections due to its sensitive nature. Indian law must explicitly define **biometric data** as **sensitive personal data** to ensure it is afforded the same level of protection as health, racial, or political data under the **DPDPA**.

2. Lack of Comprehensive Consent Mechanisms

Biometric systems often fail to provide clear, **meaningful consent**. Under current laws, such as the **Aadhaar Act** and **BIPA**, consent is required but is often obtained in ways that do not empower users to make informed decisions. For instance, biometric consent is typically bundled with other agreements or forced upon individuals as a condition for accessing essential services, such as welfare programs, banking, or telecommunications.

To address this, there is a need for a **reform in consent mechanisms**. This includes ensuring that consent is **freely given**, **explicit**, and **withdrawable** at any time, as prescribed by the **GDPR**. **Opt-out mechanisms** should be provided in situations where biometric data is used for non-essential purposes, and individuals must be informed of the implications of data processing. **Informed consent** must not only be theoretical but also implemented in ways that empower individuals to make autonomous choices.

3. Insufficient Data Security Measures and Accountability

Current data protection frameworks are often insufficient in mandating **strong data security measures** to safeguard biometric data from unauthorized access, breaches, and exploitation. While the **DPDPA** introduces penalties for non-compliance, there is a lack of enforceable standards for **data minimization**, **encryption**, and **deletion** of biometric data once it is no longer necessary for the original purpose.

Moreover, **accountability mechanisms** to ensure that organizations comply with data protection regulations are weak. **Biometric data controllers** should be required to demonstrate that their systems are designed with **security by design** and **privacy by design**, as outlined by the **GDPR**. Regular **audits** and **impact assessments** should be mandated to assess the risks and benefits of biometric data processing.

4. Ambiguity in Cross-Border Data Transfers

Another regulatory gap is the **lack of clear rules on cross-border biometric data transfers**. Given the global nature of biometric data processing, the **transfer of biometric data** to jurisdictions with weak data protection

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

laws poses a significant threat to privacy and security. The **GDPR** restricts data transfers to countries outside the EU unless they meet adequate protection standards, setting a strong precedent for global data governance.

In India, however, the **DPDPA** introduces the concept of **data localization** but lacks specific provisions governing cross-border transfers of sensitive biometric data. Legal clarity is needed on whether biometric data may be transferred to other countries and under what conditions. Moreover, international agreements and mechanisms should be created to ensure that biometric data is only transferred to countries that uphold comparable data protection standards.

5. Insufficient Oversight and Regulatory Bodies

There is a **lack of robust oversight and regulatory bodies** to monitor and enforce compliance with biometric data protection laws. While the **Data Protection Authority (DPA)** in India under the **DPDPA** is tasked with enforcement, there remains a gap in its ability to effectively oversee biometric data practices, especially in **public sector projects** such as **Aadhaar**. In the EU, the **European Data Protection Board (EDPB)** and national regulators have a more active role in scrutinizing data processing activities and issuing fines for violations, which serves as a deterrent.

India must establish a **dedicated biometric data regulatory body** with the mandate to oversee the development and deployment of biometric systems, investigate complaints, and enforce compliance with data protection laws. This body should also ensure that biometric systems are regularly updated to address emerging threats to privacy and security.

Proposed Reforms

To address these regulatory gaps and ensure that biometric HCIs are deployed responsibly, several reforms are necessary:

1. **Explicit Definition of Biometric Data**: Biometric data should be explicitly defined as **sensitive personal data** under the **DPDPA** and treated with the same level of protection as health and financial data.
2. **Enhanced Consent Mechanisms**: Implement **opt-in**, **informed**, and **revocable consent** for the collection and use of biometric data, ensuring that individuals can make well-informed decisions about their data.
3. **Stronger Data Security and Privacy Protections**: Enforce stronger **data security standards** for biometric data, including **encryption**, **storage limitations**, and **deletion policies** after the purpose for which the data was collected is fulfilled.
4. **Clear Rules on Cross-Border Transfers**: Establish clear guidelines for the **cross-border transfer of biometric data**, ensuring that such transfers only occur to jurisdictions with comparable data protection standards.
5. **Enhanced Oversight and Accountability**: Create a dedicated regulatory body for **biometric data governance** to monitor and enforce compliance, conduct regular audits, and issue penalties for violations.

Conclusion

Biometric human-computer interfaces (HCIs), including fingerprint scanning, iris recognition, and facial recognition, represent a rapidly advancing frontier in technology with significant implications for security, privacy, and individual rights. As these technologies are increasingly adopted across various sectors—ranging from smartphones and public services to law enforcement and healthcare—legal and ethical concerns have become more pressing. The ability to accurately identify individuals using biometric data offers profound advantages, but it also necessitates rigorous legal frameworks to prevent misuse, ensure privacy, and protect fundamental human rights.

This paper has explored the **current legal frameworks** governing biometric HCIs in key jurisdictions, including **India**, the **European Union (EU)**, and the **United States (US)**. It identified that while each jurisdiction has made strides in regulating biometric data, **critical regulatory gaps** remain, particularly in terms of **consent**, **data**

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

security, **cross-border data transfers**, and **oversight**. The **Indian legal landscape**, despite the establishment of frameworks like **Aadhaar** and the **Digital Personal Data Protection Act (2023)**, still lacks sufficient safeguards for biometric data. The **EU** has taken a more comprehensive approach through the **GDPR**, treating biometric data as sensitive and requiring strict controls, while the **US** remains fragmented with state-specific laws like **BIPA**, leaving significant regulatory uncertainty.

The **ethical concerns** surrounding biometric HCIs—such as issues of **consent**, **data breaches**, **surveillance**, **bias**, and **discrimination**—are deeply intertwined with the legal framework. Addressing these concerns requires an urgent **reform** of existing laws and a rethinking of how biometric data is collected, stored, processed, and shared. **Stronger regulatory measures** must be implemented, including clearer definitions of biometric data, enhanced security standards, mandatory impact assessments, and robust oversight bodies.

In conclusion, as biometric HCIs continue to evolve and shape the way we interact with technology, the regulatory landscape must evolve accordingly to safeguard **privacy**, **freedom**, and **equity**. Only through comprehensive reforms can we ensure that these technologies are used ethically, responsibly, and in full compliance with human rights principles. The establishment of **global standards** and stronger **international cooperation** will also play a crucial role in ensuring that biometric systems do not become tools of exploitation, but instead serve as a force for good—advancing security, convenience, and access without infringing on personal freedoms.

This research highlights the pressing need for **lawmakers**, **regulatory bodies**, and **technology developers** to work collaboratively in creating frameworks that balance the **innovative potential** of biometric HCIs with the protection of **individual rights**. As we look to the future, the legal and ethical handling of biometric data will likely remain a pivotal issue in the broader discourse on **digital rights**, **privacy**, and **human-computer interaction**.

Bibliography

Legal Materials

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, Acts of Parliament, 2016 (India).
2. Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
3. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1 (2008) (U.S.).
4. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
5. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Extraordinary, Part II, Section 3(i).

Case Law

6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Books and Academic Articles

7. ANIL K. JAIN, ARUN ROSS & KARTIK NANDKUMAR, INTRODUCTION TO BIOMETRICS (Springer 2011).
8. Ian Kerr, Biometric Surveillance and the Right to Privacy, 5 THEORETICAL INQUIRIES L. 255 (2004).
9. Emilio Mordini & Carlo Petrini, Ethical and Social Implications of Biometric Identification Technology, 43 ANN. IST. SUPER. SANITÀ 5 (2007).
10. DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE (Open Univ. Press 2001).
11. Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006).

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Reports and Policy Papers

12. Eur. Data Prot. Bd., Guidelines 05/2021 on the Use of Facial Recognition Technology in the Area of Law Enforcement (May 18, 2021), https://edpb.europa.eu.
13. NITI Aayog, Data Empowerment and Protection Architecture (DEPA) Whitepaper (2021), https://niti.gov.in.
14. Centre for Internet & Society, Privacy and the Aadhaar Project: A Critical Analysis (2018), https://cis-india.org.
15. World Econ. F., Responsible Limits on Facial Recognition Technology: Charting a Global Governance Roadmap (2020), https://www.weforum.org.

Online News Sources

16. Aadhaar Data Breach: UIDAI Faces Fresh Questions on Security, ECON. TIMES (Mar. 3, 2018), https://economictimes.indiatimes.com.
17. Will Knight, The World Is Scrambling to Regulate Facial Recognition, WIRED (July 31, 2021), https://www.wired.com.
18. Natasha Lomas, Clearview AI's Facial Recognition App Deemed Illegal in EU, TECHCRUNCH (Feb. 17, 2022), https://techcrunch.com.