Panjab University Law Magazine (MAGLAW)
ISBN: 2582-3507, Volume Iv Issue I, pp 50-67

AI IN EMBRYO SELECTION IN INDIA: BALANCING PRIVACY AND PRODUCTIVITY

Sania[*]

ABSTRACT

Embryo selection in in-vitro fertilization (IVF) involves assessing the characteristics of fertilized embryos to identify the most viable ones for transfer (in the human body) or cryopreservation which means freezing for further research. Recently, artificial intelligence (AI) has been increasingly integrated into this process to enhance accuracy and automate decision-making. However, the application of AI in embryo selection raises significant ethical and legal concerns, particularly regarding the potential misuse of sensitive genetic information. This research paper examines the risks associated with AI-driven embryo selection, focusing on the threat it poses to the privacy of the genetic information individuals undergoing IVF. The study highlights the essential features required by the legal mechanisms which are to be specifically designed in order to regulate AI systems and studies the newer legal mechanisms in the United States, European Union and India including the General Data protection Regulation[1], Digital Personal Data Protection Act[2] etc. which have been passed with the aim of safeguarding of individual privacy. It further analyses the relevant parts of these laws while also focusing on the loopholes to identify the key elements required in order for these laws to be successful in India in achieving their aims. By emphasizing on the Indian perspective to this issue, this research highlights the importance of addressing these statutory and regulatory challenges in to prevent misuse and protect the confidentiality of patients undergoing AI driven IVF in India. The findings emphasize the critical role of regulations in mitigating risks while fostering innovation in reproductive technologies.

KEYWORDS: *Artificial intelligence, Embryo Selection, Right to Privacy, Cyber laws, Digital Personal Data Protection Act, 2023*

---

[*] UILS, Panjab University, Chandigarh, B.A.LL.B. (Hons.), 6th Semester

[1] General Data Protection Regulation, 2016, European Union, *available at https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679* (last visited on March 9, 2025). [2] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

INTRODUCTION

1.1 Objectives of Study

The primary objective of this study is to explore the role of artificial intelligence in embryo selection and the associated ethical and privacy concerns. It seeks to identify the specific privacy risks linked to the use of AI in handling sensitive genetic and personal data, such as potential data breaches or misuse. By analysing existing legal frameworks in the United States, European Union and India, the study aims to highlight best practices and gaps in addressing privacy protections in this new era of AI. Additionally, it evaluates the India's current legal stance on the matter, particularly in relation to data protection laws. Ultimately, it strives to strike a balance between using AI for advancements in reproductive technologies and upholding the fundamental right to privacy, ensuring that innovation does not compromise ethical and legal principles.

1.2 What is IVF?

Fertilization occurs when a sperm (male gamete) combines with an egg (female gamete) to create a zygote, which is the first step in the formation of a new life. Once fertilization takes place, the zygote starts dividing rapidly through a process called mitosis. As it travels through the fallopian tube toward the uterus, the zygote transforms into a blastocyst—a hollow, fluid-filled structure containing a cluster of cells known as the inner cell mass, which will eventually develop into the embryo. About 5 to 7 days after fertilization, the blastocyst attaches to the lining of the uterus, a crucial step that signals the start of embryonic development.

This entire process of fertilization ordinarily takes place inside a woman's body where natural conception takes place. However, due to reasons such as blocked or damaged fallopian tubes, severe male infertility, genetic disorders, recurrent miscarriages etc. which prevent natural conception, fertilization can be made in vitro.

The phrase "in vitro" originates from Latin, meaning "in glass."[2] It refers to experiments or procedures conducted outside a living organism, usually in a lab setting, such as in a petri dish or test tube. In the case of in-vitro fertilization (IVF), it specifically means that the fertilization of an egg by sperm takes place outside the body in a controlled environment, after which the resulting embryo is transferred (placed into the uterus) or preserved for research.

---

[2] Zhou W, Gao X, Liu D, Chen X, "Gold Nanoparticles for In Vitro Diagnostics" 115 *Chemical Reviews* 10575-10636 (2015).

1.3 What is Embryo Selection?

Embryo selection in IVF involves evaluating and choosing the healthiest embryo for implantation to maximize the chances of a successful pregnancy. After fertilization, embryos are cultured for 3 to 5 days and assessed based on their growth, cell structure, and quality. Advanced techniques which are discussed further in this paper are used to screen embryos for genetic abnormalities. The best-quality embryo is then selected for transfer, while others may be frozen for future use (cryopreservation). Embryologists are specialized scientists who study and handle reproductive cells, playing a crucial role in assisted reproductive technologies like In Vitro Fertilization (IVF). They are responsible for retrieving, analyzing, and fertilizing eggs with sperm in a laboratory, monitoring embryo development, and selecting the best embryos for implantation.

1.4 Advent of Artificial Intelligence in IVF

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines, enabling them to perform tasks that typically require human cognitive abilities, such as learning, reasoning, and problem-solving. AI has transformed various industries, particularly medicine and healthcare, where it is driving innovation and enhancing productivity.

AI is being widely used to collect, store and analyse the lifestyle, health status and genetic information of patients undergoing certain medical procedures including IVF. All of this data is being compiled and linked to produce a more predictive picture of our health or medical status. Talking about India, Nova IVF Fertility, one of India's largest fertility chains, has shown interest in adopting AI technologies to improve IVF outcomes. So, it is clear that India is not far behind the developed countries when it comes to the adoption of AI in healthcare.

1.5 PRIVACY CONCERNS

The application of AI in embryo selection requires processing extensive genetic and biological data, which raises significant concerns about the security and privacy of this sensitive information. A major risk lies in data breaches and cybersecurity weaknesses, as AI systems depend on digital databases storing genetic sequences, patient medical histories, and embryo imaging. Unauthorized access or hacking could result in the exposure of highly personal reproductive and genetic details, leaving individuals vulnerable to issues like identity theft or the misuse of their genetic information. This could also lead to patients losing control over their genetic data, sparking ethical debates around consent, ownership, and the responsible use of such information.

2. RESEARCH METHODOLOGY

The present study adopts a qualitative and doctrinal research approach, relying on primary and secondary sources to investigate the use of artificial intelligence (AI) in embryo selection, its implications for privacy rights and relevant legal mechanisms. The methodology is designed to systematically collect, analyze, and interpret data from a variety of credible sources to address the research objectives. The aim of the research was to critically analyse various legal regulations which are existing based on their efficiency in regulating AI systems while also highlighting and emphasizing on important features which are required in laws and regulations which aim to ensure individual privacy in the digital world.

2.1. NATURE AND SOURCES OF DATA

The study is based on an extensive review of secondary data including publications, scholarly articles, student papers and websites. These sources provided a foundational understanding of the current applications of AI in reproductive technologies and the associated privacy concerns.

Legal Provisions were analysed through primary legal sources, such as bare acts and official government portals, were reviewed to study the statutory frameworks governing AI, data protection, and privacy in India and other jurisdictions.

2.2. ETHICAL CONSIDERATIONS

The research adheres to strict ethical standards:

1. All sources have been properly cited to ensure academic integrity and avoid plagiarism.
2. Credible and authoritative sources, such as peer-reviewed journals, official government portals, and legal documents have been used to maintain the reliability and accuracy of the study.
3. The study respects the sensitivity of the topic by focusing on ethical and legal implications without making speculative or unverified claims.

3. CONTENT ANALYSIS

3.1. PURPOSE

Content analysis was employed to systematically examine and interpret textual data from online articles, research papers, and legal documents. This method was

chosen to identify recurring themes, patterns, and trends related to the use of artificial intelligence (AI) in embryo selection and its implications for privacy rights. By analyzing the content of these sources, the study aims to provide a comprehensive understanding of the ethical, legal, and technological dimensions of the topic.

3.2. DATA SOURCES

Peer-reviewed journal articles and reputable online publications were reviewed to gather insights into the technological, ethical, and legal aspects of AI in embryo selection. Primary legal sources, such as bare acts and official government portals, were consulted to study the statutory frameworks governing AI, data protection, and privacy in India and other jurisdictions.

3.3. CODING AND CATEGORIZATION

The data was read thoroughly, and initial codes were assigned to key concepts and ideas. Further, the codes were grouped into broader themes such as ‘privacy risks,’ ‘ethical concerns,’ ‘legal frameworks,’ and ‘technological advancements.’ Finally, each theme was further divided into sub-themes to facilitate a detailed analysis.

3.4. ANALYTICAL FRAMEWORK

Thematic analysis approach was adopted to analyze the data. This involved identifying and interpreting patterns within the data, organizing the themes and sub-themes into a coherent framework and using manual coding to ensure a thorough and nuanced understanding of the data.

3.5. INTERPRETATION OF FINDINGS

The content analysis revealed several key findings including the facts that privacy risks associated with AI in embryo selection are a recurring concern across jurisdictions, ethical concerns, such as the potential for discrimination and misuse of genetic data, were frequently highlighted in the literature and gaps in India's legal framework, particularly in comparison to international standards, were identified. These findings were interpreted in the context of the research objectives, providing a foundation for the study's conclusions and recommendations.

4. ARGUMENTS AND DISCUSSIONS

4.1 Why do we need AI in IVF?

"A study titled "Embryo selection through artificial intelligence versus embryologists published in *Human Reproduction Open* in 2023 reported that AI models achieved a median accuracy of 75.5% (ranging from 59% to 94%) in predicting embryo morphology grades, surpassing the 65.4% accuracy of embryologists' assessments."[3] Multiple research studies have compared the performance of AI with embryologists and it is now well established that AI has immense potential to improve IVF success rates.

Besides, it also reduces the workload of experts and saves time and money of the healthcare providers and patients. In fact, it also saves the educational expenditure used for training students to access embryo health. This is because doctors who specialize in this procedure need years of training and practice to become embryologists and yet, are likely to make mistakes. "Interpretation of data that appears in the form of either an image or a video can be a challenging task. Experts in the field have to train for many years to attain the ability to discern medical phenomena and on top of that have to actively learn new content as more research and information presents itself. However, the demand is ever increasing and there is a significant shortage of experts in the field. There is therefore a need for a fresh approach and AI promises to be the tool to be used to fill this demand gap."[4] "AI-based embryo selection significantly reduces the time required for manual grading by embryologists, improving workflow efficiency in IVF clinics."[5] "Besides, it also lowers operational costs by minimizing human labor and reducing the need for repeated IVF cycles."[6]

The traditional method of evaluating embryo health demanded embryologists to spend a great deal of time in observing embryos and but with the intervention of AI, the job of embryologists has shifted from **'*observation*' to '*operation*'**.

---

3 Salih, M., Sergio, A. L. R., Ali, A. M., Ahmed, A. M., Salih, M. A., Mohammed, A. A., Nasr, A. A. M, "Embryo Selection through Artificial Intelligence versus Embryologists: A Systematic Review", 2023, *available at https://pubmed.ncbi.nlm.nih.gov/37588797/* (last visited on March 5, 2025).

4 Adam Bohr, Kaveh Memarzadeh (eds.), *Artificial intelligence in healthcare* (Elsevier, Amsterdam, 2020).

5 Meseguer, Marcos, José Bellver, José Remohí, Antonio Pellicer,Nicolás Garrido, "The Use of Artificial Intelligence in Embryo Selection: A Systematic Review" 42 *Reproductive BioMedicine Online* 521 (2021).

6 Bormann, Charles L., Laura M. Parikh, Amarnath G. Bhide, Marcos Meseguer, David H. McCulloh, "Artificial Intelligence in Human In Vitro Fertilization: A Review of Recent Advances" 116 *Fertility and Sterility* 876 (2021).

Now, the embryologists are to be trained to operate the AI, which does the observation and also analyses and predicts the future health of the embryos for them. All we humans have to do is to learn to operate this technology. "The rise in maternal age and associated complications such as diminished ovarian reserve and increased aneuploidy rates have contributed to the growing demand for IVF and other ART services."[7] Besides, "delayed childbearing and age-related fertility decline have resulted in more couples seeking IVF and egg freezing to overcome natural conception challenges."[8] "Additionally, the recent global COVID19 pandemic has delayed childbearing and fertility treatment for many. Thus, there will be an expected increase in demand for IVF moving forward." The current average IVF success rate is approximately 30% which means that only 30% (approx.) of the IVF cycles result in successful pregnancies. "The focus of a great deal of research is to improve the current ~30% success rate of IVF."[9] "To reduce the number of IVF cycles, diminish the risk associated with multiple pregnancy, and maximize the efficacy of IVF treatment, genetic data generated from the preimplantation genetic screenings was analysed and a prototype of an AI-assisted program was developed to evaluate the viability and quality of each embryo."[10] The intervention of AI into IVF has significantly improved this number. Therefore, it is true to say that AI has significantly improved the productivity of IVF technologies and the speed of treatments. Today, companies like Weill Cornell Medicine (United States)[11] and Harrison.ai (Australia)[12] have successfully developed such AIs and are working in assistance with multiple fertility clinics and hospitals to implement this technology in IVF. However, the next question is, is it worth the risk of letting genetic data exposed to breaches and how exactly can such data breach occur? These questions have been discussed in the next sections.

---

7 G. M Chambers, E. A. Sullivan, O. Ishihara, M. G. Chapman, G. D. Adamson, "The Impact of Maternal Age on Assisted Reproductive Technology Outcomes" 29 *Human Reproduction* 14091417 (2014).

8 T.J. Mathews, B.E. Hamilton, "Delayed Childbearing: More Women Are Having Their First Child Later in Life" 21 *NCHS Data Brief* 1-8 (2009).

9 D.J.X. Chow, P. Wijesinghe, K. Dholakia, K.R. Dunning, Does Artificial Intelligence Have a Role in the IVF Clinic?, *available at https://pubmed.ncbi.nlm.nih.gov/35118395/* (last accessed on March 7, 2025).

10 Y A Tang, S J lee, "Embryo prioritization through an AI-powered evaluation system improves the clinical outcome in IVF cycles" 39 *Human Reproduction* 201 (2024).

11 Zaninovic, Nikica, Marcos Meseguer, Carlos Simón, Jose Remohí, David B. Gardner, "Artificial Intelligence in Human Embryo Assessment: Clinical Applications and Ethical Considerations" 38 *Journal of Assisted Reproduction and Genetics* 1655 (2021).

12 Chen, Serena H., David F. Albertini, Catherine Racowsky, Marcos Meseguer, Alan H. DeCherney, "The Role of Artificial Intelligence in Modern IVF Practices" 5 *Fertility Research and Practice* 12 (2022).

4.2 How does AI in IVF risk privacy?

Right to Privacy is a widely explained concept in India and has been established by multiple interpretations and precedents, even though it has not been explicitly mentioned in the Indian Constitution. Right to privacy can be inferred from Article 21 i.e., Right to life and personal liberty.[13] The concept of right to privacy has evolved over time with the progress of society and advancements in technology. As our world has changed, this right has taken on new layers and meanings, reflecting the diverse ways in which it impacts our lives today especially with the advent of the era of internet. In the landmark case of K.S. Puttaswamy vs Union of India[16] (Adhaar Card Case), the three-judge bench held that "informational privacy is a facet of the right to privacy and dangers to privacy in an age of information can originate from both the state and non-state factors. The court also directed the Central Government to put a robust regime for data protection in the same case."

The importance of safeguarding privacy rights has only made itself more prominent with the increasing usage of internet throughout the world and whenever there is a new technological advancement, there is a new facet added to this right. For example, social media has added a new facet to right to privacy where the users have to agree to "privacy policy" after installing most apps online by which they are agreeing to sharing of their personal details with the company.

These details are used by companies to run targeted advertisements on our screens. However, these companies have an obligation to not sell our private information to third parties and ensure safeguards to protect our information.

Similarly, with the advent of AI in the recent years, the ambit of informational privacy has broadened requiring more complex technological safeguards. Introduction of AI in general healthcare poses risk to data breach because "big data" is stored and processed by machines and this data majorly includes the general lifestyle, medical history and overall mental and physical health records of the patients. In fact, when AI is introduced in complex and sensitive procedures such as IVF, the risk is multiplied manifold as there is now the inclusion of also the genetic information of such patients. "The novel introduction of artificial intelligence into 'in vitro' fertilization technology is medically promising and ethically concerning at the same time. The new possibilities and complexities generated by involving intelligent, powerful

---

13 The Constitution of India, art.21. [16] AIR 2015 SC 3081

algorithms in human creation and reproduction, raise a host of ethical issues for IVF patients, practitioners embryologists, in particular, and society at large."[14]

However, simply speaking of data breach and privacy risk becomes pointless if there is no knowledge of the negative consequences of such breaches. So, what is the worst that could happen if our genetic information gets leaked? To answer this, we should first keep in mind that genetic data is deeply personal and unique to each individual, acting like a biological fingerprint. If this information is leaked, it can be exploited to identify or track someone without their permission. Since it is so specific, genetic data could even be used for identity theft, allowing malicious actors to impersonate someone or target them with highly personalized scams.

Similarly, insurance companies could use genetic information to deny coverage or hike up premiums if they believe someone is predisposed to certain illnesses.

Besides, genetic data does not just affect the individual, it can also reveal sensitive health information about their family members, exposing their private details without consent. This creates a ripple effect, impacting not just one person but entire families. This is not mere hypothesis and a popular example of this is the 'GEDmatch Data leak case of 2020'. GEDmatch is a popular online platform where individuals can upload their genetic data to find relatives and explore their ancestry. It gained widespread attention for its role in helping law enforcement solve cold cases, most notably the identification of the Golden State Killer in 2018. In July 2020, GEDmatch experienced a security breach that exposed the genetic data of 1.2 million users. The breach was particularly alarming because GEDmatch had previously positioned itself as a more privacy-conscious alternative to commercial genetic testing companies. However, the incident revealed that even platforms with strong privacy claims could be vulnerable to cyberattacks.[15]

---

[14] S. Tamir, "Artificial Intelligence in Human Reproduction: charting the ethical debate over AI in IVF" 3 *AI and Ethics* 947-961 (2022).

[15] P. Ney, L. Ceze, T. Kohno, Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference, Network and Distributed System Security Symposium (NDSS), San Diego, USA, Feb. 2020, *available at https://dnasec.cs.washington.edu/genetic-genealogy/ney_ndss.pdf* (last visited on March 9, 2025). [19] Korada Lakshminarayana "Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers" 11 *European Journal of Advances in Engineering and Technology* 105109 (2024).

Besides, there is also something called "Data poisoning".[19] Data poisoning is a malicious tactic where someone deliberately tampers with the information used to train machine learning systems. The attacker's aim is to sabotage the model, making it perform poorly, produce wrong results, or favor specific outcomes that serve their agenda. This kind of attack takes advantage of a critical weakness in machine learning i.e., "the models are only as good as the data they learn from". If the data is corrupted, the entire system can be compromised. "Intentionally, data poisoning can occur when data are collected from various software packages by tampering with data"[16] So, if data poisoning occurs in an AI model which is being used in IVF technology, it completely defeats the whole idea of it being more accurate and productive than embryologists.

History has witnessed that even when we strengthen technologies and make them more secure, hackers always seem to stay one step ahead. They are constantly evolving and finding new ways to bypass defenses faster than we can update our security measures. So, it is essential for specific and stringent legal mechanisms to be put in place to regulate the use of machines and reduce the risk of data breaches.

4.3 What are the existing legal mechanisms for data privacy in the European Union, United states and India, and are they sufficient?

As AI becomes more and more common in our day to day lives, laws must also evolve to regulate AI systems to ensure their safe and secure use.

As of today, there are no existing laws (other than the European Union AI Act, 2021) which specifically aim at regulating AI. However, the existing cyberlaws which have undergone multiple amendments and have been updated to fit a wide range of technologies into their ambit, can also be applied to AI due to broad definitions and interpretations. In this section, I have discussed some of the prominent legal mechanisms in the United States, European Union and India which can be molded and interpreted to fit the demands of today's times with the advancement of AI systems. But, let us first discuss the EU AI Act which specifically targets AI systems.

---

16 Y. Chen and P. Esmaeilzadeh, Generative AI in medical practice: In-depth exploration of privacy and security challenges, (2024) 26 Journal of Medical Internet Research e53008, *available at https://pubmed.ncbi.nlm.nih.gov/38457208/* (last visited on March 6, 2025).

European Union AI Act[17] is by far the only law that is made keeping AI in mind which applies to AI systems placed in the EU market or used in the EU, regardless of where the provider is based. Under this act, AI systems are categorized into four risk levels i.e., unacceptable risk (includes banned practices

> e.g., real-time biometric surveillance in public spaces), high risk (includes practices requiring strict surveillance e.g., AI in critical infrastructure, healthcare, law enforcement), limited risk (includes practices with transparency requirements
>
> e.g., chatbots must disclose they are AI) and minimal risk (including practices requiring no specific regulations e.g., AI-enabled video games). Use of AI in healthcare is included in the high-risk category. This means that healthcare providers using AI must implement risk management systems to identify and mitigate risks, high-quality datasets must be used to minimize biases and errors, detailed records must be maintained for traceability and compliance, clear and understandable information must be provided to users. Besides, the mechanisms must ensure human intervention to prevent harmful outcomes and systems must perform reliably and resist adversarial attacks. These are the basic requirements to be fulfilled for a high-risk AI system.

European Union Cyber Security Act, 2019[18] aims to strengthen the EU's cybersecurity framework and establishes the "European Union Agency for Cybersecurity" (ENISA) as a permanent body. It came into full effect in 2021, the same year when EU AI Act was also passed. While the act primarily focuses on cybersecurity certification and enhancing ENISA's role, some provisions are relevant to AI regulation, particularly in ensuring the security and resilience of AI systems. Article 2 of the act defines ICT products as "any element or group of elements of a network or information system. AI systems often consist of hardware (e.g., GPUs, specialized chips) and software (e.g., machine learning algorithms, neural networks)", which fall under the definition of ICT products as "any element or group of elements of a network or information system." Besides AI systems often operate as services that process, analyze, or transmit data, which aligns with the definition of ICT services as provided in the same article as "any service consisting fully or mainly in the transmission, storage, retrieval,

---

[17] European Parliament, EU AI Act: First Regulation on Artificial Intelligence, (2023*) available at https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulationon-artificial-intelligence* (last visited on March 6, 2025).

[18] European Union, The EU Cybersecurity Act, (2019) *available at https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=LEGISSUM%3A4398780* (last visited on March 8, 2025).

or processing of information by means of network and information systems". So, we can say that even though the Cyber Security Act was not made specifically keeping AI systems in mind, it is still relevant for regulating AI systems due to its broad definitions and interpretations.

It also provides framework for mandatory certification of ICT products and services by defining three levels of assurance for certification i.e., basic (for lowrisk systems), substantial (for systems with higher risks), high (for systems with the highest risks e.g., critical infrastructure).

Coordinating both these acts can create a system where, for AI systems being used in healthcare and qualifying as high-risk systems, it is mandatory to obtain certificate under the cyber security act and follow the requirements of high-risk systems under the AI act. This system can ensure that AI systems used for IVF undergo appropriate security checks and maintain standard safeguards to uphold patient privacy.

Now, let us discuss about the *grundnorm* which lays the foundation for Cyber laws in EU. **General Data Protection Regulation (GDPR)** is a comprehensive data protection law that governs the processing of personal data within the European Union (EU) and the European Economic Area (EEA).[19] The purpose of this regulation is to protect individuals' fundamental rights and freedoms, particularly their right to data protection, while ensuring the free movement of personal data within the EU. Article 4 of the act defines 'personal data' as "any information relating to an identified or identifiable individual" and 'processing' as "any operation performed on personal data." These definitions can easily include AI systems working in IVF. Article 6 of the act talks about the lawfulness of processing and lists the legal bases for processing personal data, such as consent, contract performance, legal obligations, and legitimate interests and Article 7 specifies that consent must be freely given, specific, informed, and unambiguous. Articles 12 to 23 grant individuals (data subjects) several rights, including: Right to access[20] (individuals can request access to their personal data), Right to erasure[21] ("right to be forgotten") i.e., individuals can request deletion of their data under certain conditions. Right to restriction of processing[22]

---

19 He Li, Lu Yu and Wu He, The Impact of GDPR on global technology development, Journal of Global Information Technology Management, *available at https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186* (last visited on March 6, 2025).

20 General Data Protection Regulation (GDPR) 2016/679, art 15, *available at https://gdprinfo.eu/art-15-gdpr/* (last visited on March 5, 2025).

21 *Id.*, art. 17.

22 *Id.*, art. 18. [27] *Id.*, art. 20.

(individuals can request limiting how their data is used) Right to data portability[27] (Individuals can request their data in a machine-readable format), etc. Therefore, GDPR acts as the baseline and grants the patients essential rights which ultimately ensure accountability and transparency of the AI system manufacturers and healthcare providers.

In the United States, **Computer Fraud and Abuse Act (CFAA)[23]** is one of the primary laws addressing cybercrime. It criminalizes unauthorized access to computer systems and networks and prohibits access to a computer without authorization or exceeding authorized access and covers a wide range of activities, including hacking, data theft, and the distribution of malware. This can be efficiently enforced to prevent hacking and data poisoning in IVF AI systems by criminalizing it. Even though this act came in 1986, (when AI was not a matter of concern) it can still be enforced to regulate AI systems and prosecute against malicious uses of AI as it forms a part of computer systems.

The **Health Insurance Portability and Accountability Act (HIPAA)[24]** in the US is also highly relevant to the regulation of AI in embryo selection, as it sets the standard for protecting sensitive patient data in the United States. When AI is used in embryo selection, HIPAA compliance becomes critical to ensure the privacy and security of patient data. According to the act, Personal Health Information (PHI)[25] includes any information that can identify an individual and that relates to their health. In embryo selection, this includes genetic data, medical histories, and treatment records. By establishes safeguards to protect the confidentiality, integrity, and availability of electronic PHI (ePHI)[31], this act can ensure safety of AI systems by preventing unauthorized access and ensuring that only authorized personnel can access PHI. There needs to be collaboration between clinics, researchers, and AI developers for avoid HIPAA violations. This creates an entire system which is aimed at providing complete security in IVF AI systems.

Talking about India, we have no legislation specifically targeting AI but the existing laws can be interpreted to include AI systems in their domain. The

---

23 U.S. Department of Justice, Criminal Resource Manual, (Computer Fraud), *available at https://www.justice.gov/jm/jm-9-48000-computer-fraud* (last visited on March 7, 2025).

24 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996), *available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW104 publ191.pdf* (last visited on March 7, 2025).

25 Steve Alder, What is Considered PHI Under HIPAA?, HIPAA Journal (2023), *available at https://www.hipaajournal.com/considered-phi-hipaa/* (last visited on March 6, 2025). 31 What is ePHI?, HIPAA Journal (2024), *available at https://www.hipaajournal.com/ephi/* (last visited on March 6, 2025).

Indian Council of Medical Research (ICMR) provides guidelines for ART but does not yet have specific regulations for AI in embryo selection.

The very well-known **Information Technology Act, 2000** [26] is the primary legislation in India governing electronic commerce, cybersecurity, and digital transactions. While the IT Act, 2000 does not explicitly address artificial intelligence (AI), its provisions can be interpreted and updated to address AIrelated challenges. It requires organizations to implement reasonable security practices to protect sensitive personal data and criminalizes activities such as hacking, identity theft, and spreading malware. It can therefore help prosecute cases of improper security measures by companies using AI in IVF and also cases of data poisoning.

Information Technology (Security Procedures) Rules, 2004: Prescribe the security procedures and practices for ensuring the integrity, confidentiality, and authenticity of electronic records and digital signatures. Electronic records can include the data store by IVF AI systems for embryo analysis. Hence, these rules can be applicable to it.[27]

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011: Mandate organizations to implement reasonable security practices to protect sensitive personal data. These rules will ensure that AI companies working in collaborations with healthcare providers and fertility clinics follow security practices while development and implementation of AI technologies for IVF in India.[28]

The latest development in digital data privacy mechanism in India is the **Digital Personal Data Protection Act (DPDP), 2023** which applies to the processing of digital personal data within India and to data processed outside India if it involves offering goods or services to individuals in India. Therefore, it becomes significant in regulating IVF AI systems in India. Section 2 of the act defines 'personal data' as "any data that can identify an individual" and 'data principal' as "the individual to whom the personal data relates".[29] The data collected by AI in IVF falls in the ambit of the definition of 'personal data' under this act and the patients under that of 'data principle.' The act also establishes the

---

26 The Information and Technology Act, 2000 (Act 21 of 2000)

27 The Information Technology (Security Procedure) Rules, 2004, *available at https://indiankanoon.org/doc/60823482/* (last visited March 3, 2025).

28 The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, *available at https://indiankanoon.org/doc/114407484/* (last visited March 3, 2025).

29 Supra note 2, s.2.

Data Protection Board of India (DPBI) as the regulatory authority for enforcing the act.[30] It imposes penalties for non-compliance, ranging from ₹50 lakh to ₹250 crore, depending on the severity of the violation.[37]

Besides, the same section also defines 'data fiduciary' as "Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."[31] In context of IVF AI systems, this will include the manufacturers of the system along with the fertility clinics or hospitals they are working in collaboration with. Obligations of Data Fiduciaries under the act include 'Lawful Processing'[32] (i.e., data fiduciaries can only process personal data for lawful purposes and processing must be done in a fair and transparent manner), 'Consent Requirement'[33](data fiduciaries must obtain explicit consent from data principals before processing their personal data.) The Consent must be informed (individuals must be aware of what they are consenting to), specific (must be given for a specific purpose), unconditional (cannot be tied to unrelated conditions).[34] Besides there are certain 'Notice Requirements' [35] to be fulfilled by fiduciaries as well. Data fiduciaries must provide a clear and concise notice to individuals, including the purpose of data processing, the types of personal data being collected, the rights of individuals under the Act.

By amending conflicting or overlapping provisions in other laws, Section 19 ensures that the DPDP Act becomes the primary legislation for data protection in India.[36] Under the IT Act, companies were liable for data breaches under Section 43A.[37] With the DPDP Act in place, penalties for data breaches will now be governed by this act, ensuring stricter and more specific consequences.

Drawing inspiration from global data protection laws like the GDPR, the DPDP Act is tailored to India's unique needs and challenges. However, while the Act has been enacted, the Data Protection Board of India (DPBI**)**, which is crucial for its enforcement, has not yet been established. Once operational, the DPBI will play a vital role in safeguarding individual privacy rights and ensuring that the DPDP Act is effectively implemented, particularly in sensitive areas like AIdriven embryo selection.

---

30 Supra note 2, s.18. 37 Supra note
31 Supra note 2, s.2(i).
32 Supra note 2, s.4.
33 Ibid
34 Supra note 2, s.6.
35 Supra note 2, s.5.
36 *Supra* note 2, s.19.
37 *Supra* note 35, s.43(A).

5. FINDINGS

1. The use of AI in embryo selection holds great promise for boosting the success rates of IVF treatments, offering hope to countless people struggling with infertility. AI can save time and money by saving expenditure on training embryologists. By analyzing complex data with precision, AI can improve outcomes and make the process more efficient. Therefore, it is true to say that there is need to introduce AI in ART.
2. Sensitive genetic and medical data must be handled with care to protect individuals' right to privacy but AI puts such data at risk. It exposes the data to hackers which can lead to Cyber Crimes. Besides, the AI giants collecting such information can potentially misuse the data and profit out of it.
3. In the European Union, The EU AI Act and EU Cyber Security Act can work alongside each other and with GDPR acting as the *grundnorm* to ensure that individual privacy is of utmost priority.
4. In the US, CFAA and HIPAA together can be used as weapons against malpractices in AI run IVF technology. However, there is scope for AI specific regulations in the US.
5. In India, the Digital Personal Data Protection Act (DPDP Act), 2023 is well-equipped to address the privacy challenges associated with AI systems in IVF through measures like data encryption, informed consent, and strict access controls. While this law provides a solid foundation, introducing AI-specific regulations in the future could further strengthen the framework, addressing unique issues like algorithmic bias and ensuring that innovation in IVF remains ethical, secure, and aligned with India's constitutional values.

6. CONCLUSION AND SUGGESTIONS

AI in embryo selection holds significant promise for enhancing the success rates of IVF treatments. However, its adoption also raises critical privacy concerns, necessitating the legal frameworks to strike a balance between innovation and ethical considerations. Existing legal mechanisms in India, if enforced properly, can sufficiently address AI-related challenges and will play a vital role in ensuring that advancements in AI are harnessed responsibly, safeguarding both productivity and ethical standards. The Digital Personal Data Protection Act (DPDP Act), 2023, can serve as a starting point by requiring measures such as data encryption, informed consent, and strict access controls. In future, we might need tailored regulations for healthcare and assisted reproductive technologies to address specific issues, like how genetic data is stored and shared. Ensuring transparency in how AI algorithms work, conducting regular audits, and setting up an independent body, can also help maintain accountability. By taking these

steps, we can create a system that supports innovation in embryo selection while safeguarding individual privacy rights.

SUGGESTIONS AND RECOMMENDATIONS:

1. Set Up a Central Ethics Committee for AI in Fertility Treatments

To ensure that AI is used responsibly in fertility care, we should form a dedicated oversight committee. This group would bring together diverse voices of ethicists, doctors, legal experts and AI specialists to guide fair and transparent decision making.

2. Update Fertility Laws to Include AI Safeguards

India's ART (Regulation) Act, 2021[38] should evolve with technology. Clear rules on AI in fertility clinics for covering patient data security, algorithmic fairness, and rights protection would help prevent misuse.

3. Keep Genetic Data Secure Within India

Genetic information is deeply personal. To prevent misuse, India could require specific laws and regulations to ensure that embryo-related genomic data be stored locally for reducing risks of foreign exploitation.

4. Train Doctors in the Ethics of AI-Assisted Fertility

Medical professionals using AI for fertility treatments should be educated on its ethical challenges like bias in algorithms and patient privacy so that they can make informed and compassionate decisions while respecting patient privacy.

5. Educate Patients on AI's Role in IVF

Many people undergoing IVF may not fully understand how AI impacts their treatment. Public awareness campaigns can empower them with knowledge which while help in ensuring informed decisions.

6. Rigorous Enforcement of Digital Personal Data Protection Act (DPDP), 2023 in Fertility Clinics

It would be key to mandate strong encryption, strict access controls, and secure storage for genetic data. Beyond legal formalities, clinics should prioritize

[38] V.D.S. Jamwal, A.K Yadav, "The Assisted Reproductive Technology (Regulation) Act, 2021: A Step in the Right Direction" 48 *Indian Journal of Community Medicine* 4-6 (2023)

transparency, explaining in clear terms how AI tools use personal data, so consent is truly informed rather than just a signed form. Regular audits and meaningful penalties for breaches will keep clinics accountable, turning data protection laws into real-world safeguards for patients. If proper safeguards like these are taken, India can advance its assisted reproductive technologies with AI while ensuring protection of the fundamental right to privacy.