INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"REGULATING EMOTIONAL SURVEILLANCE: A LEGAL FRAMEWORK FOR AI-BASED EMOTION RECOGNITION"

AUTHORED BY - SAKSHI TRIPATHI, MANAN JHAMB & VAISHNAVI MISHRA

ABSTRACT

Police agencies and companies are employing artificial intelligence (AI) that includes emotion detection systems to identify mental states in the tone of voice and facial expressions. These kinds of approaches pose large moral and legal issues, particularly relating to privacy and consent. The Indian Supreme Court has declared the right to privacy a fundamental right. It was historic. However, "emotional data" is not defined from the privacy perspective. But feelings are quick to change, are situational, and are often extremely personal, so the collecting of them is very irritating. Emotional AI doesn't work the same for everyone, and there are legal loopholes where bias and abuse could creep in. The paper concludes that emotion data should be recognized as part of informational privacy by the law and that it should be subject to stringent purpose limitation and informed consent.

KEYWORDS: Emotional AI, Privacy, Consent, Bias, and Informational Privacy.

INTRODUCTION

The area of artificial intelligence (AI) has rapidly evolved from processing data to encompass systems that can interpret emotions in body language, facial expressions, and changes in speech. This tendency, sometimes called "emotional surveillance," makes us think hard about privacy, liberty, and the moral boundaries of modern technology. More and more organizations, schools, police departments, and even grocery stores are deploying emotion recognition systems, promising to be more efficient and customized for each person. But as they are bothersome and can be used in the wrong way, they should be looked at by the law straight away. Emotional surveillance probes people's feelings more than other sorts of monitoring. This paves the way for manipulation, discrimination, and loss of their dignity. The lack of a functioning legal framework makes these risks much worse. Data security rules now mostly deal with personal data, but they don't do enough to secure affective data.

ISSN: 2582-6433

UNDERSTANDING AI-BASED EMOTION RECOGNITION TECHNOLOGIES

AI-based emotion identification works by computers observing a person's facial expression, voice, and body language to determine their mood. These technologies are based on computer algorithms that mimic the brain and learn to function with lots of data, such as photographs of faces, noises, or portions of the body. AI systems attempt to categorize emotions into joyful, angry, fearful, and sad. In order to achieve this, they seek subtle signals such as modest facial expressions, changes in vocal tone, or variations in heart rate.

The foundation of emotion recognition is affective computing, the first field that connected human emotions to machine reactions. Some are speech analysis tools that examine pitch and rhythm, face recognition algorithms that plot facial landmarks, and sensor-based systems that measure how the body reacts. Increasingly, people are combining various inputs in a multimodal approach for improved results. A system might prevent choosing the erroneous one by looking at voice tone and facial emotions at the same time.

The range of applications for these technologies is expanding rapidly. They are used in classrooms to detect how engaged pupils are; in workplaces to see how healthy people are; in police work to spot stress or lying; and in consumer markets to make marketing more appropriate to each person. However, mood recognition is still disputed, despite its potential. Emotions are subjective, culturally complicated, and situationally dependent. To grin in some cultures implies enjoyment; in others, courtesy. That makes it difficult to group all of the things together.

Also, the training data that these systems learn from don't often contain much variety. This can result in biases that impact minority groups more than others. It also raises ethical concerns about permission, manipulation, and monitoring. On the other hand, there is emotional data that invades the private domains of the mind of individuals, creating difficulties of autonomy and respect.

"The next big thing is going to be AI-based technologies that connect people and machines and understand how they feel," he said. But before we can utilize them, there have to be severe restrictions concerning them. Complex regulations are needed to hold people accountable and

ISSN: 2582-6433

to examine new ideas, to protect people from harm, and to ensure that basic rights are protected.

THE NATURE OF AFFECTIVE DATA: PRIVACY AND AUTONOMY CONCERNS

1. Defining Affective Data

Associative data is information about how people feel, what they believe, and how they talk. Things like voice tone, face emotions, body language, and even physical signals like heart rate can tell you a lot. Personal data like a person's name, age, or where they live can be used to find them, but affective data gets under their skin. That shows. People have strong feelings about themselves. Such private information is protected under "Article 21"[1] of the Constitution of India. It asserts every person has a right to life, personal liberty, and privacy, as decided in Justice K.S. Puttaswamy v. Union of India[2].

2. Sensitivity of Emotional Information

Emotions are not merely fleeting responses; they are about what it means to be human and to be individual. Affective data can be used wrongly and leave openings that can be used or controlled. For instance, corporations monitoring their workers' emotions can penalize them for stress or sadness. The Supreme Court in the Puttaswamy case has held that protection of mental and emotional states is a part of privacy. This means that affective data is particularly sensitive and requires more legal protection.

3. Privacy Concerns in Collection

One major issue is that emotional data is often obtained without clear consent. Cameras at public locations, schools, or workplaces can observe face expressions without the watched knowing. This makes our globe a "surveillance society" in which people are continually under monitoring. Such acts are against the principle of informed consent, which is protected under Indian privacy legislation and the "Digital Personal Data Protection Act, 2023"[3]. Coercive emotional surveillance without authorization infringes on the constitutional right to privacy.

4. Risk of Misinterpretation

[1] Constitution of India 1950, art 21
[2] Justice K.S. Puttaswamy (Retd.) and Anr v Union of India and Ors (2017) 10 SCC 1 (SC).
[3] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

ISSN: 2582-6433

But emotions are different, depending on the situation and the society. In one community a smile may mean happiness. In another, it could be politeness or unease. AI systems are susceptible to misreading emotions and drawing erroneous conclusions about intent and character. Such misperception might spoil the image of a person or even make it difficult for him/her to get a job in the multicultural culture of India. Such misrepresentation is more likely to affect persons from minority or marginalized groups and thereby undermines the promise of equality in "Article 14"[4].

5. Autonomy and Free Will

To be autonomous is to be able to decide for yourself and not have someone else decide for you. If companies or governments utilize emotional data to anticipate or manipulate people's behavior, people lose control of their decisions. Emotional nudges in politics or advertising take away people's free will and make them choose things they may not have chosen otherwise. Article 21 of the Constitution states, "Autonomy is essential for respect and freedom. The Supreme Court has emphasized this numerous times, and emotional manipulation is a blatant violation of this constitutional value.

6. Bias and Discrimination

The datasets on which emotion detection systems are trained are often not culturally diverse. This results in unfair outcomes when the feelings of people from minority countries are ignored. For example, facial recognition systems trained on datasets from the West may misinterpret the expressions of Indian individuals. Bias amplifies stereotypes. Bias is against Article 14, equal protection under the law. It also raises moral considerations about how to use technology in a fair and just way.

7. Consent and Transparency Issues

If you are indeed giving your consent, you should know what information is being collected, how it will be used, and why. But most of us don't realize we're being monitored by our thoughts. If you don't know what's going on, the guaranteed right to privacy is meaningless. The Digital Personal Data Protection Act, 2023, discusses a lot about consent, but it doesn't talk about emotional data yet. This hole allows people to be viewed voyeuristically emotionally without their knowledge, making it difficult for them to control personal information.

[4] Constitution of India 1950, art 14

ISSN: 2582-6433

8. Impact on Human Dignity

When people's sentiments become data points that are continuously being watched, human experience is less engaging. Honor is an integral part of life and liberty and is protected by Article 21. "Thoughts as things" means a good thought or a thing. Respect? I don't give a damn. Humans who wish to be treated with respect should be treated as humans, not things to be looked over. Emotional marketing may strip people of their humanity, turning them into numbers who are blind to their own value.

9. Legal and Ethical Gaps

Today's laws are about things that can be used to identify a person, such as names, locations, or financial information, not how they are feeling. Affective data is fluid and subjective and more difficult to police, which makes it susceptible to negative usage. Morals may be shifting, but Indian law needs to catch up fast to defend rights in the digital age. Without explicit norms and protections, emotional surveillance may get worse." This may violate constitutional rights to privacy, equality, and respect.

10. Need for Regulation

We need robust laws to tackle these problems. It should define emotional data, regard it as very private data, and punish people who exploit it. If you want to persuade people to agree, you've got to tell them, you've got to watch over them, and you've got to balance new ideas with the protection of essential freedoms. The GDPR in the EU offers privacy protections for biometric and psychological data that can serve as a model for Indian law. Regulations need to preserve privacy, autonomy, and dignity, yet also enable responsible AI development.

CONCLUSION FOR NATURE

Emotional data is no different from any other personal data. It lets you glimpse inside our minds. Its gathering and use raise serious questions about privacy and freedom. Emotional surveillance might lead to a society in which individuals are being monitored and controlled all the time, and if AI gets their sentiments wrong, they are to blame. Also, in this age of AI, it is necessary to preserve personal data under Article 21 and make sure that everybody has the same rights under Article 14. This is a good approach to defend freedom and honor. The law of the future must be able to combine modern technologies with constitutional standards so that people's rights are respected and not violated.

ISSN: 2582-6433

COMPARATIVE LEGAL PERSPECTIVES: GLOBAL APPROACHES TO EMOTION RECOGNITION

There are currently no worldwide standards for AI-based emotion identification, but significant players such as the EU, US, China, and Japan have chosen diverse paths, from risk-based frameworks to sector-specific regulations. India's new law on data security is only just beginning to get a grip on sensitive data.

1. European Union: Risk-Based Regulation

The EU's AI Act is risk-based and classifies emotion recognition as a "high risk" application when it is utilized in sensitive areas such as education, law enforcement, or the workplace. This will imply more stringent standards on accountability, transparency, and human monitoring. The EU includes emotional data inside its GDPR requirements. The EU considers biometric and psychological data to be sensitive and does not allow processing without explicit consent.

2. United States: Sector-Specific and Litigation Driven

The US has no comprehensive AI legislation. Instead, emotional AI is regulated in different ways by different kinds of legislation—consumer protection laws, job laws, and privacy regulations. The Federal Trade Commission (FTC) has issued a warning about using emotion recognition in deceptive and dangerous ways. Class actions and lawsuits are increasingly significant enforcers of laws, particularly when emotional AI leads to discrimination or privacy violations.

3. China: State-Driven Oversight

On the matter of laws for AI, China is strongly committed to state control and safety. Many utilize mood identification for spying, teaching, and other reasons. To achieve the aims of national security and social safety, businesses must follow the rules set by the government. Less about preserving people's privacy More about ensuring emotional AI aligns with government interests.

4. Japan: Ethical Guidelines and Industry Standards

Japan has started to use "soft laws" and has issued ethical guidelines for the use of AI. In the health and elder care sector, you develop emotional awareness but with respect for the rights

ISSN: 2582-6433

and culture of the person. The Japanese model relies on voluntary compliance and industry norms, not severe regulatory requirements.

5. Canada: Human Rights Lens

In Canada, mood recognition is currently legally regulated by human rights and privacy regulations. The Privacy Commissioner's Office is concerned about emotional data, as it could be deployed to infringe on fundamental rights to equality and privacy. Canada takes a fair and balanced approach to AI.

6. India: Emerging Frameworks

Affective data in India is governed by the Digital Personal Data Protection Act, 2023, which does not explicitly regulate tracking of emotions. The Constitution, in Article 21, says that people have the right to freedom and privacy. This is reiterated in the case of Union of India v. Puttaswamy. The law is still uncertain, although the court can also examine effective evidence.

7. Comparative Risk-Based vs. Rights-Based Models

While the EU model is risk-based, the approaches in India and Canada are rights- based, emphasizing respect and freedom. In the US, it's lawsuits; in China, it's state interests first. Such differences indicate the influence of political and cultural background on norms.

8. Transparency and Consent Standards

There is a common thread globally of consensus and transparency. The EU demands explicit agreement for affective data, whereas Japan advocates transparency via moral values. On the contrary, the framework of China does not lay too much value on individual permission, which shows the difference of China's beliefs in governance.

9. Accountability Mechanisms

Accountability is made in different ways in different areas. The EU has human control and audit trails, the US has lawsuits and FTC action, and Japan has self- regulating enterprises. The monitoring systems under India's DPDP Act are still being built up, and so there are still gaps in the utilization of them.

10. Future Directions

There will probably be some worldwide agreement on high risk, classification, openness, and

ISSN: 2582-6433

justice, but there will still be some disagreement due to cultural and political differences. A viable option for India to govern emotional monitoring would be a hybrid model combining the risk-assessment paradigm of the EU with protections for constitutional rights.

AI DETECTING EMOTIONS IN HIRING AND POLICING

1. How AI Emotion Detection Works

Artificial intelligence systems evaluate human behavior by using body language, tone of voice and facial expressions. These systems analyze large quantities of data with the help of machine learning algorithms to detect patterns and classify them into categories like happiness, anger, fear or sadness. For example, a change in the tone of speech may indicate nervousness, while a raised eyebrow may be perceived as astonishment. Technology appears clever. But emotions are very subjective and influenced by culture, situation, and individual differences. This makes emotion recognition far less reliable than more traditional biometric data like fingerprints or iris scans. Courts across the globe have recognized the limitations of these technologies. For example, the case of **State v. Loomis (Wisconsin, 2016)**[5] addressed algorithmic prejudice in criminal justice, which has similarities to the problems of emotion detection in sensitive scenarios.

2. Use in Hiring

Some firms are starting to trial emotion recognition systems during job interviews. These AI algorithms scan a candidate's tone of voice or facial expressions for attributes such as passion, honesty or confidence. The idea is to make hiring more 'objective' and reduce human bias. But there could be problems because of it. A candidate who displays concern can be perceived as dishonest, while a reluctant candidate might be perceived as unenthusiastic. There are other complications caused by cultural variations. In certain cultures, a serious face is a show of respect, not apathy. Bias is not absent in emotion recognition and the emotional data might be unfairly penalizing for applicants and bias reinforcing. Privacy and autonomy are basic rights recognized in Indian jurisprudence under Article 21, as notably enunciated in **Justice K.S. Puttaswamy v. Union of India (2017).** The use of emotional data in hiring processes without informed consent may breach these rights.

3. Use in Policing

[5] State v Loomis, 881 NW 2d 749 (Wis 2016)

ISSN: 2582-6433

Law enforcement agencies in numerous countries are trialling emotion recognition to detect stress, fear or dishonesty during questioning or surveillance. The hope is that AI would be able to notice suspicious activity faster than people can. For example, police could deploy emotion recognition cameras in public spaces to identify persons who appear to be terrified or anxious. However, it is normal to be frightened when the police are about and does not necessarily suggest that you are guilty. Misreading emotions might lead to wrong targeting, harassment or even arrests. In law enforcement, where the repercussions can be life-altering, reliance on defective AI systems creates serious ethical and legal difficulties. The Indian Supreme Court in **Selvi v. State of Karnataka (2010)**[6] held that involuntary narco analysis and lie detector tests infringed on the right to self-incrimination in Article 20 (3). Law enforcement's emotion recognition suffers similar difficulties in that it trespasses into people's minds without their consent.

4. Privacy and Autonomy Concerns

Emotion identification reveals much more sensitive information about a person's sentiments than a name or fingerprint. In a "surveillance society" people lose their private feeling when continually monitored at work, in interviews and public areas. Moreover, the ability to make choices for oneself is diminished. People may adapt their public behaviors to avoid being flagged and candidates may feel compelled to "perform emotions" for AI systems. This undermines the free choice and dignity, which are ideals enshrined in Puttaswamy and safeguarded by Article 21 of the Indian Constitution. In **Peck v. United Kingdom (2003)**[7]**,** the European Court of Human Rights ruled that the surveillance was a breach of human rights since it was a 'intrusion without justification into private life'. Monitoring one's inner states to detect emotions might violate these standards.

5. Legal and Ethical Issues

The ability to discern emotions varies from country to country. The EU's AI Act puts emotion recognition in the 'high risk' category. It has to follow strict rules on obligation, transparency, human oversight and more. In the United States, regulation is piecemeal and mostly the product of consumer protection laws and litigation. Much expression recognition is used to instruct and spy on people and China is very focused on state control. India's Digital Personal Data Protection Act, 2023 does not refer to emotional data per such, but does lay out requirements

[6] Selvi v State of Karnataka (2010) 7 SCC 263 (SC)
[7] Peck v United Kingdom (2003) 36 EHRR 41 (ECtHR)

ISSN: 2582-6433

for processing personal data. Courts have acknowledged privacy and autonomy as fundamental rights however the law is ambiguous. However, without stringent regulation there is plenty of scope for bias, misinterpretation and abuse, especially in sensitive areas such as employment and policing. India can draw lessons from the laws in other countries such as the "EU's GDPR rules"[8] on protecting private data.

IS EMOTIONAL DATA PART OF PRIVACY UNDER K.S. PUTTASWAMY V. UNION OF INDIA?

1. Privacy in *K.S. Puttaswamy vs. Union of India*

The Supreme Court established privacy as a basic right under Article 21 of the Constitution in 2017. Crucially, the judges said that privacy is not limited to private locations such as your house but also includes your personal autonomy, dignity, and control over your information. That implies privacy protects what you do and what data about you is collected.

2. Informational Privacy

One of the key contributions of the verdict was the recognition of informational privacy. In the digital age, personal data may tell us intimate things about people. The court observed that people should have the right to choose:

- What information is being shared about them?
- With whom it is shared,
- What it is used for,

This includes sensitive categories such as health records, financial information, and psychological or emotional data.

3. Emotional Data and Its Nature

Emotional data is data about a person's feelings, moods, stress, or psychological states. It can be derived from facial recognition, voice analysis, biometric sensors, and even social media interaction.

- **Deeply personal:** Why emotional data is intimate and core to human identity, unlike basic demographic data (age, gender).

[8] https://business.gov.nl/regulations/protection-personal-data/?gad_source=1&gad_campaignid=23285156368&gbraid=0AAAADAUIc9RO65v-yPSRyseO2vWhIH_S&gclid=CjwKCAjwtIfPBhAzEiwAv9RTJkaslbxJ7h-8QWguaxqSSJOg4qIt9nCEN520CyI0noQ_GqFTZZY1YBoCh-kQAvD_BwE

ISSN: 2582-6433

- **Potentially revealing:** May expose vulnerabilities, mental health issues, or personal preferences.
- **Connected to dignity:** Emotional data protection is a precondition to safeguard human value, as dignity is at the heart of Article 21.

4. Risks of Emotional Surveillance

The Court in *Puttaswamy* warned against unchecked data collection. Emotional data is especially risky because

- **Profiling:** Companies or governments could categorize people based on emotions (e.g., anxious, angry, happy).
- **Manipulation:** Advertisers or political actors could exploit emotional states to influence decisions.
- **Discrimination:** Employers or institutions could use emotional monitoring to judge performance or loyalty unfairly.

Thus, emotional data requires strong constitutional protection.

5. Autonomy and Emotional Data

Autonomy is the ability to make free decisions in one's life. Because emotional data is strongly related to autonomy:

- It is a reflection of mental processes and sentiments.
- If managed by others, it can hinder self-expression and free decision-making.
- This protects individuals in their ability to control their own identity and personal story.

6. The Threefold Test from *Puttaswamy*

The Court has devised a way to determine whether state interference with privacy is lawful:

1. **Legality:** The invasion must be legal.
2. **Legitimate Aim:** A fair target. The law has to help individuals to attain a worthy goal, such as safety.
3. **Proportionality:** Influence must be required and not excessive. For mental data, it means the following:
   - You can't secretly see how people are feeling.
   - It must have a clear legal purpose.
   - It has to be good for everybody.

ISSN: 2582-6433

- It should not violate the tight requirements.

7. Emotional Data as Part of Informational Privacy

The judgment made it plain that privacy encompasses both decisional liberty (what you eat, who you marry, your sexuality) and informational privacy (management over your data).

Emotions data is both

- It's informed privacy since it's information about the way someone thinks and feels.
- It is a part of decisional liberty, because feelings affect decisions, and if they are protected, people can decide freely.

8. Digital Age Concerns

The Court has seen the difficulties of the digital age. A good example is emotional data:

- **AI and Big Data:** Today, machines can sense your emotions through wearable devices or facial recognition.
- **Consent Issues:** Sometimes, too, there is the problem of consent. People don't realize their emotional information is being captured.
- **Invisible Surveillance:** Feelings can be monitored all the time, without the individual knowing. Unlike fingerprints.

Thus, emotional information is very private and is protected by the Constitution.

9. Practical Implications After *Puttaswamy*

- **Data Protection Laws:** India is tightening rules such as the Digital Personal Data Protection Act, 2023, to protect personal data. It is assumed that emotional data fall under "sensitive personal data."
- **Consent:** For any collection of emotional data, informed permission is needed.
- **Restrictions on monitoring:** The proportionality test means employers, schools, or the government can't track people's feelings.

NO CLEAR INDIAN OR GLOBAL DOCTRINE

When we claim there is "no clear Indian or global doctrine," it indicates there is no concept or framework that is widely acknowledged and that applies consistently across all contexts. A doctrine in law and policy typically helps to provide guidance, set limits, and ensure consistency of interpretation. But in many areas from international relations to constitutional law and new

ISSN: 2582-6433

areas like technology regulation countries and courts go different ways. For example, India may refer to its constitutional provisions and court precedents, while global institutions or other countries may adopt very different norms. One lack of settled doctrine leads to doubt. This gives flexibility but also means that the results rely on the jurisdiction, context, or interpretation. In practice this often results in discussions, diverging opinions, and problems harmonizing rules internationally. Scholars and practitioners say that the absence of a defined doctrine harms consistency and predictability and makes it harder to resolve disputes or develop long-term policies. At the same time, the lack of a strict doctrine may also foster innovation and adaptation, since judges and policymakers are allowed to interpret principles in light of changing social, political, and technological circumstances. Thus, the phrase points to both a weakness, lack of clarity and uniformity and a strength space for evolution and diversity of ideas. It just implies that there is no one set guiding concept that India and the globe have agreed upon yet. There is room for many interpretations, and the argument is still on.

CONCLUSION

The results indicate that the use of AI to identify emotions, in the context of emotional tracking, raises serious concerns about privacy, autonomy, and dignity. Emotional data is very private, flexible, and culturally sensitive; thus, it can be dangerous to misuse it. These instruments should not be abused or misused and should be regulated in some way. This is especially the case in sensitive areas such as employment and law enforcement. In the Puttaswamy case, the Indian Supreme Court ruled that freedom and privacy were essential rights. Feelings are also granted these rights. Indian laws don't cover private data, especially the Digital Personal Data Safety Act, 2023, and there is a safety gap. The EU has strict risk rules, but China is state-controlled. This is an example of how culture and politics may change the rules. India needs both constitutional protection and risk-based requirements. Finally emotional.

REFERENCES

WEBSITES

- https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
- https://business.gov.nl/regulations/protection-personal-data/?gad_source=1&gad_campaignid=23285156368&gbraid=0AAAADAUIc9RO65v-yPSRyseO2vWhIH_S&gclid=CjwKCAjwtIfPBhAzEiwAv9RTJkaslbxJ7h-

ISSN: 2582-6433

8QWguaxqSSJOg4qIt9nCEN520CyI0noQ_GqFTZZY1YBoCh-kQAvD_BwE

ACTS

- The Indian Constitution Act
- Digital Personal Data Protection Act, 2023