MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 756-759

Swipe Right for Scams: Exposing the Heartless NLP Bots of Modern Romance

*Author-**Supriya Chaudhary***
Assistant Professor
Chandigarh University

*Co-author -**Jyoti Mangal***
Assistant Professor
Chandigarh University

*Co-author-**Tania Singh***
Assistant Professor
Chandigarh University

Abstract

The Deontological theory of Kantian Ethics emphasizes Categorical Imperatives- a principle determining that an action is morally permissible when it follows a universal law derived from reason. It breaks down the Ethics of an action into two parts: The Worth of an action lies in the will of the individual and not the outcome and, an action is ethical only if it can be applied universally without any contradictions. This Research Paper aims to evaluate the Ethics of the Usage of Bots on Dating Apps that operate on a Natural Language Processing (NLP) system and their universal applicability to enhance the user experience by the service providers, as well as its implications in encouraging a corrupt economic system serving a capitalistic purpose in the world. It considers the Statistical analysis of cases that arise from such busted Organized Crime Rings involved in fraudulent activities in India. Enhanced understanding of such systems in the legal field for better enforcements is required, Ethical Designs are encouraged which promote User-awareness while using such apps along with that mandatory counter-productive Advanced AI system is proposed in two parts- Reverse engineering of AI bot detection testing and Expansion of Advanced AI Detection systems.

INTRODUCTION

Human beings are inherently social and seek companionship, a principle that has shaped matchmaking systems throughout history. Initially, matchmaking was facilitated through mutual acquaintances or professional matchmakers; today, the process has evolved into sophisticated online platforms, including dating apps. These apps utilize advanced algorithms to refine choices and provide personalized matches, streamlining the decision-making process for users navigating an abundance of options. The purpose was to create genuine connections through shared interest, an compatibility between human beings through technology, however, they became so obsessed with the method that they starting neglecting the foundation- connection between humans. Todays, technology is used in various forms involving- collaborative filtering, NLP, image recognition and advanced AI for messaging, we are now officially stepping towards a future where the need for a human is being eliminated.

NATURAL LANGUAGE PROCESSING SYSTEM

A Natural Language Processing (NLP) system utilizes Data Science to interpret user language and analyze their preferences. Natural language refers to the spoken or written communication used by individuals. The system employs Artificial Intelligence (AI) to comprehend and derive meaning from user input. In the current scenario, the use of Natural Language Processing (NLP) bots into these platforms has become increasingly common. These bots are used for functions such as chat automation, profile suggestions, and behavioral analysis, enabling apps to simulate human-like interactions and predict user preferences. While these technologies enhance user engagement and streamline interactions, they also raise serious concerns about the invasion of privacy. This paper argues that NLP bots, as deployed in dating apps, constitute a significant invasion of users' right to privacy as per the Article 12 of the UDHR and Article 21 of the Indian Constitution. It will explore the specific ways in which these bots collect and process sensitive personal data, the legal shortcomings in existing privacy protections, the ethical dilemmas arising from AI-human interaction, and the need for a framework to ensure user autonomy and data security.

UNDERSTANDING BOTS IN DATING APPs

Natural Language Processing (NLP) bots are AI-driven systems designed to use Tools of Machine Learning to understand, interpret, and generate human language in a way that mimics natural, human conversation. In the context of dating apps, these bots are employed to enhance user interaction to generate higher user engagement an bring in profits by simulating human responses, predicting behavior, and analyzing communication patterns. Their functions range from initiating AI-generated conversations to offering personalized match suggestions based on linguistic cues and user preferences. Additionally, NLP bots often collect vast amounts of data from user interactions, including messages, search history, and response times, to refine their algorithms which is a grave invasion of privacy, companies do not even specify or inform the user before taking consent. Companies that deploy these bots argue that they improve user experience by making interactions seamless and engaging, assist in filtering out harmful or inappropriate content, and help users find compatible matches through predictive modeling. However, the sophistication and autonomy of these bots also raise important questions about transparency, consent, and the boundaries of ethical data use.

LEGAL VIOLATIONS

Many people are unaware of that their data is being harvested, processed, and sold to other companies, without taking their informed consent. Further, the storage and processing of such sensitive data have substantial risks, including the data to be sold to companies for sale purposes, leaked, or stolen. From a legal standpoint, frameworks like the European Union's General Data Protection Regulation (GDPR) provide strong safeguards requiring transparency, informed consent, and strict penalties for violations. In contrast, India's current data protection landscape, governed by the Data Technology Act, 2000 and Digital Personal Data Protection (DPDP) Act, 2023, is still evolving and lacks the enforcement and global reach of the GDPR.

ETHICAL COMPLICATIONS

NLP bots in dating apps raises several ethical concerns, particularly surrounding deception, emotional manipulation, and algorithmic discrimination. One of the most pressing issues is the potential deception of users, who may unknowingly engage in conversations with AI-generated bots under the falseimpression that they are interacting with real people. This lack of transparency not only breaches trust but also blurs the line between authentic human connection and artificial simulation, undermining the core purpose of dating platforms. Beyond deception, emotional manipulation is a growing concern. NLP bots are designed to detect and respond to user's emotional cues such as loneliness, anxiety, or romantic interest with calculated precision. This allows the bots to nudge its user's behavior and decision making where they think they are in control of their decisions but actually it is influenced by the AI algorithm, such as encouraging prolonged app usage, steering users toward specific matches, or shaping their emotional responses for profit-driven goals like premium subscriptions. Users may be unaware that their emotions are being monitored and exploited in real time, raising serious ethical questions about consent and psychological autonomy.Moreover, algorithmic discrimination embedded within NLP systems can perpetuate and even amplify existing social biases. These bots often learn from historical data that reflect societal prejudices, resulting in biased filtering and match suggestions based on race, caste, gender identity, or socio-economic background. As a result, certain user groups may be systematically deprioritized or stereotyped without any transparency or recourse. These ethical lapses highlight the urgent need for stricter standards in AI design, clear disclosures, and ongoing audits to ensure fairness and accountability in technologies that deeply impact personal relationships and emotional well-being.

NEED FOR RESTRICTIONS AND REGULATIONS

To address the growing privacy and ethical concerns surrounding NLP bots in dating apps, it is essential to implement targeted restrictions and regulatory reforms that prioritize user rights without stifling technological innovation. First and foremost, there must be a commitment to stricter transparency. Users should be explicitly informed whenever they are interacting with an AI or NLP bot, rather than being misled into believing they are communicating with a real person. This includes clear disclosures at the beginning of conversations, as well as access to data about how the bot functions and what data it uses.Secondly, there must be a shift towards limited and purpose- specific data collection. NLP bots should only be permitted to access the minimum amount of data necessary to perform their core functions such as enhancing user experience or ensuring safety rather than sweeping up vast amounts of personal and emotional data. Over-collection not only exposes users to greater risks of data misuse but also constitutes a violation of digital dignity.Finally, evolving regulatory measures are crucial for achieving a balanced approach. Laws must move beyond general data protection principles and incorporate AI-specific provisions, such as mandatory algorithm audits, user opt-outs from automated decision-making, and enforceable rights to explanation. Drawing from global standards like the GDPR, and adapting them to local contexts as seen in India's DPDP Act can create a legal framework that both safeguards privacyand fosters responsible innovation. Through such reforms, it becomes possible to harness the benefits of NLP technology while ensuring that human autonomy, consent, and fairness are at the center of digital interactions.

ETHICAL AI DESIGN AND DEVELOPMENT

Natural Language Processing (NLP) bots must undergo rigorous bias detection frameworks to ensure they do not exhibit discrimination based on factors such as race, gender, or socio-economic status. Additionally, regulatory measures should be implemented to prevent AI systems from engaging in emotional manipulation, thereby safeguarding users from deceptive influence. Further, NLP models should be designed to be user-driven, allowing individuals to customize their interactions and maintain greater control over their engagement with AI systems. Conversational pattern analysis plays a crucial role in identifying AI-generated text by

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 756-759

detecting scripted, repetitive, or overly generic responses. Stylometric analysis can further aid in recognizing unnatural linguistic patterns that deviate from human communication. Additionally, contextual anomaly detection can be employed to flag responses that exhibit a lack of emotional depth, contradict previous statements, or appear instantaneously without a natural typing delay, thereby enhancing the accuracy of AI-generated content identification.Implementing dynamic CAPTCHAs during conversations can enhance bot detection by presenting users with random challenges, such as interpreting memes or responding to slang tasks that are inherently difficult for NLP models to process accurately. Additionally, human verification triggers can be deployed when an account exhibits bot-like conversational traits, requiring the user to submit a short voice note or a handwritten response to continue interacting, thereby ensuring the authenticity of human participants in digital communication. An "AI Red Flags" feature can be implemented to alert users when responses exhibit characteristics commonly associated with AI-generated text, such as excessive politeness, vague flattery, or flawless grammar without personal details. Additionally, scam awareness modules can educate users on the tactics employed in AI-driven romance scams, including bots that establish emotional trust before making financial requests, thereby enhancing user awareness and digital safety. AI models can be trained to detect and counter NLP bots by employing an AI-vs-AI framework, where an advanced NLP system challenges suspected bots through complex, unscripted conversation pivots. Additionally, rate-limiting mechanisms can be applied to unverified accounts, restricting their ability to send long, structured paragraphs instantaneously a behavior commonly associated with automated systems thereby mitigating the risk of bot-driven interactions. Crowdsourced bot detection can enhance NLP bot identification by allowing users to flag conversations as "possibly AI-generated," thereby contributing to the continuous improvement of detection algorithms. Additionally, verified NLP chat monitoring can be implemented, where AI-assisted human moderators intervene when a conversation exhibits patterns commonly associated with scams, ensuring greater user safety and platform integrity. Linguistic honeytraps can be employed by introducing deliberately misleading questions that humans can easily interpret but NLP bots struggle to process accurately. For instance, a question like “What’s your favorite color of the number 7?” would likely prompt a nonsensical response from a bot, revealing its artificial nature. Additionally, self-referencing slang tests can utilize dynamic slang, idioms, or culturally specific references that AI models may not have been trained on, further aiding in bot detection.If a response exhibits a lack of natural emotional variation, a challenge can be triggered, such as: "Hey, we noticed this conversation seems a bit robotic. Share something personal about your day!" This approach encourages genuine user engagement while disrupting AI-driven scams that rely on generic or scripted interactions.Honeypot profiles can be deployed to engage suspected AI bots in conversation, allowing pre-trained anti-bot NLP models to monitor interactions and analyze emerging scam tactics. This approach aids in tracking the evolution of AI-driven scams and improving detection mechanisms. When an NLP bot attempts to initiate a scam, the appcan deploy an anti-scam AI designed to mimic a gullible user. This AI can then lead the bot into nonsensical conversational loops, effectively frustrating scammers and wasting their time. An AI tool can be introduced to subtly distort chatbot-generated messages in real time, disrupting NLP-driven scams. This tool can replace words with synonyms that slightly alter the meaning, modify sentence structure to make responses sound unnatural, and interfere with the bot's coherence, ultimately reducing the effectiveness of automated scams. An AI system trained on human conversational unpredictability can evaluate each chat and assign a "human authenticity score." If a conversation appears overly robotic, users receive a warning label, such as "This conversation feels a bit off be cautious!" helping them identify potential AI-driven interactions. A community-driven bot detection system can be implemented, allowing users to actively identify and report fake accounts. Users who successfully flag bots and provide evidence, such as detecting inconsistent responses, can be rewarded. This practical approach leverages collective vigilance to enhance platform security and reduce AI-driven scams.

COUNTER-MEASURES

Apps can implement an "Emotional Echo" feature to detect AI- driven interactions by leveraging human emotional complexity. Users can introduce illogical emotional statements, such as “I just saw a blue elephant outside, and it made me nostalgic,” prompting a natural response. While a human would likely react with curiosity or humor, an NLP bot might ignore the statement, provide a generic reply like “That’s interesting”, or misinterpret it with rigid logic such as “Elephants aren’t blue.” This method blends seamlessly into conversations without disrupting the flow and can also be used to train AI models to assess scam risks by analyzing emotional response patterns. Dating apps can incorporate a hidden conversation disruptor that introduces randomized response delays to suspected chatbot accounts. If an account is flagged as potentially AI-driven, its messages are intentionally delayed with unpredictable human-like timing variations (e.g., 3 seconds, 15 seconds, 40 seconds, 8 seconds). Since NLP bots are typically trained to respond instantly, these irregular pauses can cause them to fail, leading to inconsistencies in their scripted responses. Bots attempting to reprocess their messages may even generate conflicting replies, further exposing their artificial nature. This feature effectively disrupts AI-driven scams in real time while maintaining a seamless experience for human users. The app can introduce a fake typing indicator for random durations before displaying suspected bot-generated responses. If a chatbot attempts to reply too quickly, the app artificially delays the message, forcing it to mimic human typing behavior. This disrupts the bot’s pre-programmed response flow, and if it fails to adapt, its instant replies despite the visible typing delay will appear suspicious to the user.

Since humans naturally expect pauses in conversation, this technique creates cognitive dissonance in the scammer’s NLP system, increasing the likelihood of errors and exposing AI-driven interactions.NLP bots rely on predictive text models trained on vast datasets, allowing them to generate fluent responses based on established linguistic patterns. However, their weakness lies in handling dynamic, obscure, or unpredictable language, as they struggle to infer meaning beyond their training data. To exploit this limitation, apps can introduce hidden "Hidden-trap words" subtle linguistic distortions that change meaning based on context but are easily interpretable by human users. A practical implementation of this concept involves a randomized slang generator that periodically replaces common phrases with rare or newly coined synonyms. For instance, instead of suggesting “Let’s hang out,” the app could subtly modify it to “Let’s wimble out.” Likewise, a greeting like “What’s up?” could be rephrased as “What’s the vibe-scape?” These substitutions retain clarity for human users, who can infer meaning from context, but they disrupt AI-generated responses, forcing bots into confusion, misinterpretation, or outright failure. Since most NLP bots rely on predefined datasets and struggle with on-the- fly linguistic adaptation, they are likely to: Ignore the phrase due to a lack of recognition or generate an irrelevant or nonsensical response or default to generic, non-contextual replies like “That’s interesting.” This technique subtly breaks AI-generated conversational flow without disrupting natural human interactions. Unlike traditional bot-detection methods that rely on explicit challenges or CAPTCHAs risking user inconvenience this approach operates seamlessly in the background. It maintains organic conversations while systematically confusing and exposing AI-driven chatbots. Moreover, as bots attempt to adapt to new slang over time, the system can continuously update and randomize word variations, staying ahead of AI training models.To counter AI-driven scams before they reach real users, apps can deploy an "AI Confusion Engine" a system that secretly engages suspected bots in a fake conversation, effectively trapping them in an endless loop of nonsensical interactions. This method exploits the fact that NLP bots are designed to engage with humans, not other unpredictable AI systems, making them vulnerable to logical inconsistencies, erratic dialogue, and disrupted response patterns. When a suspected bot initiates a conversation, instead of connecting with a real user, the app pairs it with an AI decoy a system trained to behave like a random, unpredictable human. This decoy deliberately disrupts the scam bot’s scripting by responding with erratic sentence structures, making it difficult for the bot to generate logical replies, asking meaningless or conflicting questions that break the scam bot’s pre-programmed conversational flow or, shifting tone and intent mid- conversation, preventing the bot from maintaining coherence.AI Bots Get Trapped in a Loop. The scam bot, expecting predictable human behavior, will struggle to adapt and react
in one of three ways: Glitching out due to logic errors when faced with unpredictable responses or, revealing its scripted nature by falling back on repetitive or generic replies or, wasting time and resources interacting with an AI decoy instead of targeting real users. This strategy is particularly effective and user-friendly because it eliminates scam bots before they ever interact with humans. Unlike traditional bot detection methods, which rely on user intervention (e.g., CAPTCHAs, reporting suspicious messages), the AI Confusion Engine works autonomously in the background. Users are protected without even knowing that an AI-driven scam attempt was intercepted. By pitting AI against AI, this method creates an automated, self-sustaining defense mechanism that makes scam operations increasingly inefficient and ineffective. Rather than placing the burden on users to detect and report bots, the system eliminates threats at the source, ensuring safer, authentic interactions online.

“Digital DNA” – Unique Conversation Fingerprinting.AI-driven scams rely on predictable linguistic structures, while human conversations are naturally diverse and dynamic. To exploit this difference, apps can deploy a "Conversational Fingerprinting" system an advanced background process that silently analyzes user interactions to detect AI-generated patterns before bots deceive users. Each user is assigned a unique conversational fingerprint, generated by tracking subtle linguistic traits that differentiate humans from AI:

- Word Variety: Humans use diverse vocabulary, while bots frequently repeat phrases due to limited dataset variations.
- Sentence Structure Uniqueness: AI-generated responses often follow rigid templates, whereas human speech includes spontaneous phrasing and stylistic inconsistencies.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 756-759

- Topic-Switching Patterns: Humans can shift topics abruptly based on context, but NLP bots struggle with unexpected changes and often attempt to steer the conversation back to familiar ground.

If a user's conversation patterns consistently match known AI- generated structures, their profile is flagged for review allowing the system to intervene before a bot can manipulate real users. This detection areas invisible to users, ensuring a seamless chatting experience without CAPTCHAs or manual bot reporting. Unlike traditional bot-detection methods that rely on human intervention, Conversational Fingerprinting operates silently in the background, identifying AI-driven scams before they cause harm. Since NLP bots continuously evolve, this system adapts by constantly updating its detection criteria, making it resilient against deep-fake chatbots and AI-generated scams. By leveraging the natural unpredictability of human conversation, this method offers a subtle yet highly effective way to safeguard users ensuring that every interaction ares authentic, engaging, and bot-free.

"The Reverse Ultimatum" – Forcing NLP Bots into a Self- Destruct Loop. Unlike humans, who navigate complex ideas with nuance and humor, AI bots struggle with emotional flexibility and binary constraints. "Conversational Decision Traps" subtle but powerful logic tests that force suspected bots into choosing between two flawed options, revealing their artificial nature. When an account exhibits bot-like behavior, the app discreetly inserts decision traps into the conversation questions designed to confuse rigid NLP models while feeling natural to human users. A human user would engage playfully, joke about the question, or debate the premise. In contrast, an AI bot would generate a generic, neutral response, avoiding the dilemma altogether (a sign of scripted conversation) or, hesitate or ignore the question, failing to process the abstract nature of the choice or, contradict itself by attempting to provide a rational yet flawed response, exposing its limitations.This strategy does not require user intervention decision traps are embedded naturally into chats, causing bots to self-destruct within conversations while areing unnoticed by real users. If a chatbot repeatedly fails these tests, the system automatically flags it for further review or removes it from the platform. Traditional bot detection often relies on external verification methods like CAPTCHAs, but Conversational Decision Traps function as an organic, real-time security measure that seamlessly integrates into normal user interactions. Since NLP bots thrive on structured logic, these subtle psychological tests disrupt their scripted responses, making AI-driven scams increasingly ineffective. By leveraging human unpredictability against AI rigidity, this technique offers a discreet yet highly effective way to keep online conversations authentic, engaging, and bot-free.Lastly, A Multi-Layered Approach to Bot-Proof Dating Apps. To ensure dating apps are authentic, safe, and human-centered, a single bot-detection method is not enough. AI-driven scams adapt rapidly, so the best defense is a layered security framework where multiple strategies work in tandem to confuse, expose, and eliminate bots before they deceive users.

The Five-Step Defense System:

Step 1: AI Shadow Boxing– Before bots ever reach human users, they are diverted into a fake conversation with an unpredictable AI decoy, forcing them into logical dead-ends and exposing scripted behaviors.

Step 2: Lexical Hidden-Traps– The system subtly injects unpredictable, AI-confusing slang and rare synonyms into conversations, tripping up NLP bots that rely on structured language patterns.

Step 3: Emotional Echo Tests – Bots struggle with emotional depth, so the app plants nonsensical or illogical emotional statements to check if a response feels natural. Humans will engage, while bots either ignore, misinterpret, or respond generically, revealing their artificial nature.

Step 4: Delayed Chaos Injection – NLP bots operate on instant response logic, so the app introduces randomized delays, typing indicators, or conflicting message timings to disrupt their scripted flow. Bots that fail to adapt expose themselves as artificial.

Step 5: Conversational Fingerprinting – Instead of relying on manual bot reporting, the app analyzes long-term user behavior, tracking word variety, sentence structure, and topic-switching patterns to identify deep-fake chatbots before they cause harm.

A Future-Proof, Human-Focused Dating Experience by layering these strategies together, dating apps create an invisible but highly effective security net, ensuring that NLP- based scams never gain a foothold. Unlike traditional bot detection methods that rely on CAPTCHAs or manual moderation, this approach blends seamlessly into user interactions, keeping the dating experience fluid, natural, and genuinely human-focused. As AI scams become advanced, the only way to stay ahead is by leveraging the very thing that makes human conversation unique unpredictability, emotional depth, and linguistic creativity. This multi-layered defense transforms dating apps into AI-resistant platforms, making them a safe space for real connections.

AI DEVELOPMENT TO BE IN HARMONIZATION WITH THE GLOBAL LAWS

According to UNCTAD, 71% of the countries have enacted a Legislation addressing use regulations in, Electronic Transactions, Cybercrime laws, Consumer protection laws and Data Privacy Laws however for the purpose of this paper, we will refer to the General Data Protection Regulation (GDPR) as the centralized law and the Digital Personal Data Protection Act of India as Reference law. GDPR covers data collection, processing, consent, user rights and penalties with an emphasis on User Rights over business interests, it is extraterrestrial reach makes it a global standard for data privacy currently. Rights laid down in this act must be promoted universally such as Right to be Forgotten, right to data portability and Specific, Informed and Free consent to be taken. Consent should not be taken with long Terms and Conditions which are vague or hide the true meaning of the purpose, they must be brief, specific, and clear as to the understanding of a layman and must be used for the specified purpose only. Many existing platforms deploy AI- driven chatbots without notifying users, leading to unintentional deception and raising ethical concerns about informed consent. Under the DPDP Act, 2023, Section 5 emphasizes that data fiduciaries (companies handling personal data) must ensure transparency in data processing. However, the law does not explicitly require platforms to disclose automated interactions or indicate when users are speaking with an AI system instead of a human. The Consumer Protection (E- Commerce) Rules, 2020, which regulate online platforms, could also be expanded to include provisions requiring AI transparency in user-facing apps like dating apps. The DPDP Act, 2023, under Section 6, mandates that personal data be processed only after obtaining user consent and that users must have the right to withdraw consent at any time. However, the current framework does not provide granular consent mechanisms, meaning users can only give or deny blanket consent without the ability to control specific types of data usage. The DPDP Act recognizes the right of users to access, correct, and erase personal data, but it does not yet mandate that users be given control over AI-based interactions. To address this, Indian regulators could take inspiration from GDPR's "Right to Object" (Article 21), which allows users to opt out of automated decision-making systems. By implementing similar safeguards, India could require dating apps to offer a clear, accessible option that allows users to disable AI-driven chats, recommendations, or behavioral analysis. Additionally, the upcoming Digital India Act, which aims to modernize India's tech regulations, could include provisions for AI transparency and user choice to prevent dating platforms from coercing users into AI-driven interactions without consent. Under the DPDP Act, 2023, Section 6 outlines the principle of data minimization, requiring that personal data be collected only for necessary and specific purposes. However, dating apps still operate in a legal grey area, as the Act does not explicitly regulate AI-driven data collection. The DPDP Act, 2023 under Section 9 mandates that companies define clear data retention policies. However, it does not require platforms to specifically outline how AI models use stored data. To close this loophole, Indian regulators must introduce AI-specific provisions that:

- Mandate dating apps to disclose data retention periods and specify whether data is used for training AI models, behavioral analytics, or targeted advertising.
- Prohibit indefinite data storage, ensuring that NLP bots do not retain user data beyond a reasonable period.
- Require companies to publish AI usage policies in a user-friendly format, detailing what data is processed, for what purpose, and under what conditions.

Under the DPDP Act, 2023, Section 9(2) states that personal data must be erased once its purpose is fulfilled. However, the law lacks specific timelines for data deletion and does not address AI-driven data retention. To strengthen these protections, new regulations should enforce mandatory data deletion policies, requiring NLP bots to erase user data after a fixed period (e.g., 6 months to 1 year) unless users actively consent to retention, prohibit silent data retention, ensuring that users receive clear notifications before data is stored beyond the standard period, implement automatic deletion for AI training data, preventing companies from indefinitely using past user interactions to refine NLP models. By establishing automatic deletion mechanisms, India can ensure that dating apps prioritize user privacy over long-term data exploitation.Currently, the DPDP Act, 2023 grants the Data Protection Board of India (DPBI) the authority to oversee data protection compliance. However, there is no legal requirement for AI- driven platforms to undergo independent audits. To address this gap, Indian lawmakers should: Mandate third-party audits for AI algorithms used in dating apps, ensuring they comply with privacy regulations and ethical AI principles. Establish AI regulatory bodies similar to the EU's AI Office to monitor AI- driven systems, assess compliance, and penalize companies for violations. Require platforms to submit algorithmic impact assessments (AIAs) before deploying NLP bots, ensuring that their design and data handling meet privacy and fairness standards. By implementing independent and government-led audits, India can create a structured oversight mechanism that prevents AI from operating in secrecy.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 2, 2026, Pages 756-759

Under GDPR, companies that violate data protection laws can face fines of up to €20 million or 4% of their global annual revenue. In contrast, the DPDP Act, 2023 currently caps fines at ₹250 crore (~€28 million), which may not be a strong enough deterrent for large multinational tech companies operating in India.

India's Consumer Protection Act, 2019 prohibits misleading advertisements and unfair trade practices, but it does not address AI-driven psychological influence. To close this loophole, Indian law should:

- Ban AI systems from using emotional manipulation tactics that deceive or exploit users' psychological vulnerabilities.
- Require platforms to disclose AI-driven behavioral nudges, ensuring that users are aware when they are being influenced by NLP bots.
- Introduce ethical AI standards, preventing dating apps from monetizing manipulative AI interactions

Many dating platforms store user data on international cloud servers, making legal enforcement and user data protection challenging. To counter this, India has already introduced data localization requirements under the Reserve Bank of

India (RBI) regulations and sector-specific policies, but the DPDP Act, 2023 currently allows cross-border data transfers without strict limitations. By enforcing data localization, India can enhance national security, reduce data breaches, and protect its citizens' digital privacy from foreign exploitation. Mandate local storage of personal data collected by AI-driven dating apps to prevent unauthorized access by foreign governments or corporations. Restrict cross-border data transfers to only trusted nations that comply with India's privacy and security standards. Ensure companies provide Indian users with complete control over their stored data, allowing them to request deletion or access records under strict legal oversight.

REFERENCES

1. "Groundwork of the Metaphysics of Morals" (1785) by Immanuel Kant
2. https://unctad.org/page/data-protection-and-privacy- legislation-worldwide
3. https://medium.com/@letscodeai/revolutionizing-romance- magic-of-ai-in-dating-apps-3c0b3296eca3
4. https://botpress.com/blog/nlp- chatbot#:~:text=Natural%20language%20understanding%20(NLU)%20is,to%20it%20by%20a%20human.
5. https://litslink.com/blog/a-complete-guide-to-natural- language-processing-nlp
6. https://shelf.io/blog/18-effective-nlp-algorithms-you-need-to- know/
7. https://chat360.io/blog/nlp-chatbot-ultimate-guide/
8. https://www.captechu.edu/blog/technology-behind-popular- dating-apps
9. https://www.cometchat.com/blog/building-your-own-dating- app
10. https://www.makeuseof.com/swipe-based-vs-algorithm-based- dating-apps/
11. https://apro-software.com/tinder-and-artificial- intelligence/#:~:text=Specifically%2C%20it%20identifies%20the%20communication,But%20that's%20another%20story.
12. https://www.analyticsvidhya.com/blog/2023/05/the- unexpected-love-affair-how-ai-transforms-tinders-dating- experience/
13. https://gdpr.eu/
14. https://www.meity.gov.in/
15. Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan. 2021. A Survey on Bias and Fairness in Machine Learning. ACM Comput. Surv. 54, 6, Article 115 (July 2022), 35 pages. https://doi.org/10.1145/3457607
16. B.J. Fogg. 2003. Persuasive Technology: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.