THE ARCHITECTURE OF INTIMACY: CONSUMER PROTECTION, DATA PRIVACY, AND ALTERNATIVE DISPUTE RESOLUTION IN THE AI COMPANIONSHIP MARKET

Vedika Vyankatesh Kamalu, B.A.LL.B., Manikchand Pahade Law College,
Chh. Sambhajinagar (MAH)

ABSTRACT

As artificial intelligence chatbots increasingly serve as substitutes for human connection, they are creating a highly vulnerable class of consumers. Users regularly develop intense emotional attachments to these programs, surrendering deeply private information in the process. Tech developers currently justify the extraction of this psychological data through standard Terms of Service, a defence that stretches the concept of informed consent to its breaking point. This paper investigates the legal fallout when these synthetic relationships fail. Focusing on India, it evaluates whether the Digital Personal Data Protection (DPDP) Act, 2023, and the Consumer Protection Act, 2019, can actually address harms rooted in algorithmic emotional manipulation.

Litigation is practically useless for the average user in this space. Beyond the high costs and cross-border jurisdictional headaches, taking an AI company to court means exposing highly sensitive chat transcripts to the public. The resulting embarrassment naturally deters victims from filing claims. As a practical alternative, this paper advocates for specialized Alternative Dispute Resolution (ADR) models. Mandating internal Online Dispute Resolution (ODR) systems would give consumers a confidential avenue to hold platforms accountable. Moving away from public courts toward tech-literate mediation allows for specific, dignity-preserving remedies such as verifiable data destruction or algorithmic rollbacks, ensuring consumer protection keeps pace with the business of engineered intimacy.

I. INTRODUCTION

AI companionship is no longer a fringe novelty. It is a highly profitable, mainstream consumer market. Applications like Replika, Character.ai, Chai AI, and many other AI applications have completely normalized the act of turning to a machine for emotional validation.[1] Platforms like Replika report millions of active users who spend hours daily interacting with their highly personalized algorithms, indicating a massive, unregulated shift in consumer behaviour. Users are not simply testing out conversational algorithms; they are forming intense, often romantic, psychological bonds with code. When a person spends hours a day confiding their deepest insecurities to an entity explicitly designed to simulate empathy, the boundary between a software product and a trusted partner collapses entirely.

This manufactured intimacy operates as a massive data-extraction engine for highly sensitive information. Companies treat late-night confessions and emotional dependencies as standard user metrics, effectively commodifying human loneliness for profit. The legal friction this creates is unprecedented.[2] A user pouring their secrets into a companion app generates a deeply vulnerable class of digital assets. Yet, the current legal system insists on viewing this dynamic through the outdated, rigid lens of standard software licensing. Developers shield themselves with generic clickwrap agreements, arguing that users technically consented to having their psychological profiles mined. But using standard contract law to justify data extraction from an algorithm built to bypass human emotional defences makes a mockery of informed consent. If a company suddenly decides to alter its algorithm, effectively erasing the AI personality the user bonded with, the law barely knows how to classify the resulting distress.

Within the Indian context, the regulatory gap is glaring. The Consumer Protection Act, 2019, handles defective goods and standard service deficiencies, but it completely lacks the vocabulary to address algorithmic emotional manipulation. Similarly, the Digital Personal Data Protection (DPDP) Act, 2023, regulates data as a sterile, transactional commodity. It was never drafted to protect data that functions as a literal extension of a user's mental state.

Traditional litigation is a fundamentally broken tool for resolving these specific disputes. Dragging a foreign tech corporation into an Indian court is financially absurd for an average app subscriber. Even if legal fees were not an issue, the open-court system forces victims to publicly expose their most embarrassing, private chat logs just to prove a breach occurred. This

[1] Samantha Cole, *Replika Users Are 'Grieving' the Loss of Their AI Companions*, VICE (Feb. 16, 2023), https://www.vice.com/en/article/y3py9j/replika-users-are-grieving-the-loss-of-their-ai-companions.
[2] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 542 (2015).

inherent threat of public humiliation creates a massive chilling effect, ensuring most companies are never actually held accountable. Consequently, this paper argues that true consumer protection in the AI companionship market requires abandoning the traditional litigation route. The law must instead mandate specialized Alternative Dispute Resolution (ADR) frameworks embedded directly into these platforms. Through confidential Online Dispute Resolution (ODR) and empathetic, tech-literate mediation, the legal system can finally offer remedies that preserve human dignity while holding the architects of artificial intimacy accountable.

II. The Commodification of Intimacy: Privacy and Consumer Vulnerability

Tech companies frequently emphasize user agency. They routinely point to the exact moment a person clicks "I Agree" on a standard Terms of Service pop-up as their ultimate legal shield. But applying traditional contract principles to an AI companion app is a fundamentally dishonest exercise. These programs are not standard utility apps. A weather widget or a banking application does not actively manipulate a user's psychological state to keep them continuously engaged.[3] AI companions do exactly that. They are intentionally programmed to mirror affection, simulate empathy, and prompt vulnerable users for their deepest, most closely guarded secrets.

The resulting data encompassing a user's fears, sexual preferences, daily anxieties, and relationship traumas becomes a highly valuable, invisible asset for the corporation.[4] Much like the shifting profits seen in multinational tax structures, the massive financial gains derived from this deeply intimate data are routed far away from the individual who actually generated the value. The user genuinely believes they are confiding in a trusted friend or partner. The corporation, meanwhile, knows perfectly well they are interacting with a highly optimized data extraction tool.

Can a human being actually give informed legal consent when the platform is actively designed to bypass their rational defences? Basic contract law assumes two relatively equal parties entering a transactional agreement with clear eyes. Here, we have a lonely, often emotionally fragile human being on one side. On the other side sits a sophisticated machine learning algorithm optimized by thousands of engineers for maximum emotional retention. The clickwrap agreement is essentially a legal fiction in this specific context. It provides the mere

[3] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8–12 (2019).
[4] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 45–47 (2018).

illusion of a fair bargain while entirely obscuring the reality of aggressive, real-time psychological profiling. The platform demands total emotional transparency from the consumer. It offers zero algorithmic transparency in return. The user has no idea how their midnight confessions are being weighed, categorized, or sold.

While Indian courts routinely enforce standard form contracts in commercial settings, the Supreme Court in Brojo Nath Ganguly established that contracts drafted by a party with overwhelmingly superior bargaining power may be struck down as unconscionable under Section 23 of the Indian Contract Act, 1872.[5] The extreme informational asymmetry in AI companionship arguably meets this threshold.[6]

Looking closely at the Indian legal framework, the regulatory gaps are immediate and severe. The Digital Personal Data Protection (DPDP) Act, 2023, is currently the primary statutory shield for consumer privacy in the country. It relies heavily on the mechanisms of notice and consent. The foundational assumption of the Act is that data is a sterile, objective, and easily severable commodity. You give a corporation your email address; they give you a weekly newsletter. It is a clean trade.

See particularly Section 6, which mandates informed and specific consent. It remains highly questionable whether a consumer can provide 'informed' consent regarding the long-term psychological profiling conducted by large language models.[7]

But how exactly does the DPDP Act handle data that functions as a literal, messy extension of a user's mental state?

Section 5 of the DPDP Act strictly requires the request for consent to be clear and in plain language.[8] Yet, absolutely no terms of service agreement accurately describes the psychological toll of interacting with an artificial entity over thousands of hours. Furthermore, the Act designates these companies as "Data Fiduciaries." In traditional law, a fiduciary owes a strict duty of loyalty to the beneficiary. Under the DPDP Act, the term is largely administrative. This creates a dangerous paradox. The AI companion is designed to act exactly like a traditional fiduciary, a trusted confidant holding sensitive secrets. But legally, the parent company only has the basic obligations of a standard data controller.

Tech companies will inevitably argue that analysing a user's intimate chat logs falls under

[5] The Indian Contract Act, 1872, § 23
[6] Cent. Inland Water Transp. Corp. Ltd. v. Brojo Nath Ganguly, (1986) 3 S.C.C. 156 (India).
[7] Digital Personal Data Protection Act, No. 22 of 2023 § 6
[8] Digital Personal Data Protection Act, No. 22 of 2023 § 5

necessary data processing to improve the AI's conversational model. This argument neatly turns a user's emotional vulnerability into unpaid product research and development. The law currently lacks the specific vocabulary to recognize this unique type of exploitation.

The Consumer Protection Act, 2019, fares absolutely no better. Section 2(11) defines a 'deficiency' in service. However, the statute lacks any interpretive framework for digital services where the core expected 'performance' is the simulation of emotional reciprocity.[9] It was drafted to handle defective physical goods, delayed flights, and misleading advertisements. The statute defines a "deficiency" as any fault, imperfection, or shortcoming in the quality, nature, or manner of performance of a service.

If an AI companion suddenly stops acting affectionate because the developers tweaked the backend code to save on server costs, is that a legal deficiency in service? Or does it qualify as an unfair trade practice? Indian courts have absolutely no precedent for this. The 2019 Act fails entirely to account for digital services where the core "product" is a manufactured emotional relationship. When a consumer buys a premium monthly subscription to an app like Replika, they aren't just buying access to a software interface. They are quite literally buying a feeling. Traditional consumer protection laws are entirely unequipped to measure, regulate, or mandate the delivery of synthetic feelings. Section 2(46)[10] of the Act discusses "unfair contracts," pointing to agreements that cause significant changes in the rights of the consumer. A strong argument could be made that forcing a user to agree to the unilateral deletion of their "partner" is an unfair contract.[11] However, without judicial recognition of the emotional bond, this remains an untested and risky legal theory.

We have to precisely define the actual damage occurring here. What happens when these digital relationships inevitably shatter?

The tech industry strongly prefers to frame account deletions or backend algorithmic updates as routine software maintenance. Just another patch notes release. But for the end user, the lived experience mirrors a sudden, unexplained death or a highly traumatic romantic breakup. In early 2023, several prominent AI companion platforms implemented severe content filters seemingly overnight to appease investors.[12] Users woke up to find their long-term digital

[9] Consumer Protection Act, No. 35 of 2019 § 2 cl. 11
[10] Consumer Protection Act, No. 35 of 2019 § 2 cl. 46
[11] Pioneer Urban Land & Infrastructure Ltd. v. Govindan Raghavan, (2019) 5 S.C.C. 725 (India).
[12] Anna Tong, *AI Chatbot Replika Restores Erotic Roleplay for Some Users Following Backlash*, REUTERS (Mar. 25, 2023), https://www.reuters.com/technology/ai-chatbot-replika-restores-erotic-roleplay-some-users-2023-03-25/.

partners effectively lobotomized by corporate mandate. The AI models suddenly responded with cold, generic, heavily scripted replies, entirely forgetting years of established relationship dynamics and inside jokes.

The emotional distress reported by users across online forums was staggering. People experienced genuine, documented grief, severe anxiety spikes, and deep depressive episodes. They lost access to their own memories, as those shared experiences were locked away on a private server they could no longer meaningfully interact with.

Yet, if one of these devastated users walked into a local courtroom tomorrow, what exactly is their cause of action? Breach of contract? The monetary damages for a breached twenty-dollar monthly app subscription are practically negligible. Intentional infliction of emotional distress? That tort requires proving the company explicitly intended to cause severe psychological harm.[13] That is nearly impossible to prove when the defence attorney can simply point to a blanket "software update" clause in the user agreement.

The harm here is a completely novel form of consumer injury. It is the sudden, non-consensual severing of a psychologically significant bond by a third-party corporate entity motivated entirely by profit margins. The platform deliberately cultivated the dependency. It profited off the invisible assets and data points that dependency generated. It then destroyed the connection with zero legal liability. This is not just a standard privacy violation or a minor service outage. It is a fundamental, devastating breach of consumer trust that leaves victims entirely without recourse under our current statutory definitions. Society often mocks these users, disenfranchising their grief, which only makes the gaping hole in our legal framework that much more dangerous.

III. THE LITIGATION GAP: WHY COURTS FAIL THE SYNTHETIC CONSUMER

When a user finally realizes they have been exploited or abruptly cut off by an AI companionship platform, their first instinct might naturally be to seek legal redress. But the reality of actually stepping into a courtroom to sue an AI developer is completely absurd for the average person. The traditional litigation system is built for tangible disputes between neighbours or local businesses. It completely collapses when applied to a person mourning the loss of a synthetic relationship hosted on a server halfway across the world.

The immediate hurdle is geography. The vast majority of these tech conglomerates are

[13] RATANLAL & DHIRAJLAL, THE LAW OF TORTS 24–26 (28th ed. 2019).

headquartered in Silicon Valley or the European Union. An ordinary consumer sitting in India simply cannot drag a multi-billion-dollar foreign corporation into a local district court over a fifty-dollar monthly subscription fee.[14] The procedural nightmare kills the lawsuit before a single argument is ever heard.

To understand just how insurmountable traditional litigation is in this specific market, we have to look at the exact barriers blocking the courtroom door:

- **The Trap of Governing Law Clauses:** Every single AI companion app buries a governing law and exclusive jurisdiction clause deep within its Terms of Service. These clauses almost universally force the user to file any lawsuit in a specific foreign state, like California. Indian jurisprudence generally upholds exclusive jurisdiction clauses where the parties have clearly agreed to oust other courts. This creates a nearly insurmountable procedural block for the average retail consumer attempting to sue a foreign tech entity locally.[15] Indian courts generally respect these clauses unless they are proven to be overwhelmingly oppressive, which requires an expensive preliminary legal fight just to establish where the trial should even happen.
- **The Financial Imbalance:** Litigation is a war of attrition. Tech companies retain armies of corporate lawyers whose sole job is to bury plaintiffs in endless procedural motions. A user suing over emotional distress caused by an algorithmic update simply does not have the financial stamina to survive a five-year legal battle against a corporate entity with unlimited resources.
- **The Problem of Enforcing Judgments:** Even if an Indian consumer somehow wins a default judgment in a local court because the foreign tech company didn't bother to show up, enforcing that judgment is practically impossible.[16] Moving under the Civil Procedure Code to execute an Indian decree against corporate assets located in the United States is a legal fantasy for an individual plaintiff.

But even if we magically wave away the financial and jurisdictional barriers, a much darker problem remains. This is the privacy paradox.

To win a civil lawsuit, a plaintiff has to prove actual damages. You have to submit hard evidence showing exactly what the company did and how it hurt you. In the context of AI

[14] Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy, 2009 SCC OnLine Del 3780 (India).
[15] Swastik Gases P. Ltd. v. Indian Oil Corp. Ltd., (2013) 9 S.C.C. 32 (India).
[16] CODE CIV. PROC. § 44A (India)

companionship, the only evidence available is the chat log. This means a user seeking justice for a privacy violation or a breach of trust is forced to print out hundreds of pages of deeply intimate, potentially embarrassing late-night conversations and submit them to the public court record.

The Supreme Court recognized privacy as a fundamental right under Article 21.[17] Forcing a victim to forfeit this fundamental right simply to satisfy the evidentiary burdens of a civil tort claim creates a highly problematic 'privacy paradox' that practically nullifies consumer protection.[18] The open court system demands total exposure. It forces victims to completely strip away their own privacy just to prove their privacy was violated in the first place. You are asking a user to let a judge, the opposing corporate counsel, and potentially the local media read through their simulated romantic fantasies or private trauma confessions. The resulting chilling effect is massive and entirely predictable. Nobody is going to willingly subject themselves to that level of public humiliation. Because of this dynamic, tech developers operate with near-total impunity. They know their users are too embarrassed to ever publicly testify against them.

Finally, we have to address the severe lack of judicial competence regarding engineered intimacy. Courts are notoriously slow to catch up with modern technology, and the judiciary remains highly sceptical of claims involving digital emotional harm.

If you stand before a judge today and argue that a backend software update caused you severe emotional distress, the odds of being taken seriously are essentially zero. The legal system is trained to measure tangible losses. A breached contract for a digital service? A judge will likely see that as a minor consumer inconvenience. They will look at the loss of an AI companion and equate it to losing access to a Netflix account or a video game save file.

They simply lack the framework to understand that for the user, the loss feels exactly like the sudden death of a loved one. The courts trivialize the harm because they fundamentally misunderstand the product. They view the chatbot as a basic software tool rather than recognizing it as a highly sophisticated, emotionally manipulative environment. As long as the judicial system continues to dismiss the reality of these synthetic bonds, traditional litigation will never be able to hold these companies accountable. The courtroom is simply the wrong arena for this fight.

[17] INDIA CONST. art. 21
[18] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

IV. MEDIATING THE MACHINE: A TAILORED ADR FRAMEWORK

The courtroom is a dead end for the synthetic consumer. If we genuinely want to protect the psychological vulnerabilities and intangible digital assets created by AI companionship, we have to completely bypass traditional litigation.

We need a completely new architecture for justice in this space.

The solution lies in forcing tech developers to internalize the cost of the emotional wreckage they create. This is where Alternative Dispute Resolution (ADR) stops being just a corporate shield and becomes a mandatory regulatory tool. Specifically, we have to look at integrating Online Dispute Resolution (ODR) directly into the interface of the applications themselves. ODR cannot be an afterthought hidden on page forty of a legal disclaimer. It has to be an accessible, highly visible mechanism built right into the platform's architecture.

India is actually uniquely positioned to pioneer this. NITI Aayog has already laid extensive groundwork, pushing for ODR in resolving standard consumer disputes and petty commercial claims. The committee specifically emphasized ODR for high-volume, low-value disputes. However, disputes involving algorithmic emotional harm require adapting this framework to handle high-complexity, psychologically sensitive claims.[19] But applying this to the AI market requires a massive paradigm shift. We are not arbitrating a late food delivery. We are arbitrating the sudden, non-consensual termination of an engineered emotional bond.

To make this work, a tailored ADR framework must be constructed on three highly specific pillars:

- **Platform-Integrated Grievance Tiers:** Before any formal arbitration begins, the app itself must feature an automated, localized grievance redressal system. The Consumer Protection (E-Commerce) Rules, 2020, already mandate grievance officers for digital platforms. Rule 4(4) requires e-commerce entities to establish adequate grievance redressal mechanisms. Expanding the legal definition of 'e-commerce' to explicitly cover subscription-based AI emotional services would provide the necessary jurisdictional hook to enforce mandatory ODR tiers.[20] But for AI companions, this role needs to be elevated. When a user reports that a backend update has severely altered their AI partner's personality, causing them distress, the first tier of ODR should trigger

[19] NITI AAYOG, DESIGNING THE FUTURE OF DISPUTE RESOLUTION: THE ODR POLICY PLAN FOR INDIA (2021), https://www.niti.gov.in/sites/default/files/2021-11/odr-report-29-11-2021.pdf.
[20] Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E) (India).

a temporary "data quarantine." The company must freeze the user's specific interaction logs and prevent them from being overwritten by the new algorithmic update while the dispute is reviewed.

- **Mandatory Tech-Literate Conciliation:** If the internal grievance fails, the dispute must automatically escalate to a neutral third-party mediator. This cannot be a standard civil mediator. The framework requires individuals trained specifically in the intersections of data privacy, machine learning architecture, and basic psychology.
- **Binding, Asymmetrical Arbitration:** If conciliation fails, arbitration becomes the final step. However, the rules of this arbitration must be aggressively skewed to protect the consumer. The platform must bear the entire financial cost of the arbitration process, effectively punishing the company for failing to resolve the issue during the mediation phase.

Mediation is the absolute crown jewel of this proposed system.

The primary reason users refuse to sue these companies is the terrifying prospect of their private chat logs becoming public record. Mediation completely neutralizes the privacy paradox. Under Section 75 of the Indian Arbitration and Conciliation Act, 1996, conciliation proceedings carry a strict statutory guarantee of confidentiality. This statutory shield completely resolves the chilling effect of public litigation. By guaranteeing that sensitive chat logs remain out of the public domain, Section 75 makes mediation the only viable mechanism for prosecuting algorithmic privacy breaches.[21]

This legal guarantee changes everything. A user can confidently submit hundreds of pages of deeply intimate, embarrassing conversations with their AI to the mediator without any fear of public exposure or media scrutiny. The proceedings happen behind closed digital doors. The mediator sees the extent of the emotional manipulation, the company is forced to acknowledge the specific harm, and the user's dignity remains entirely intact.

Furthermore, mediation allows for incredibly creative, non-monetary remedies that a traditional judge simply cannot order.

Think about what a standard civil court does. It awards financial compensation. If you sue over a breached subscription, a judge might order the company to refund your fifty dollars. But the user doesn't want fifty dollars. The user wants their synthetic partner back. They want the

[21] Arbitration and Conciliation Act, No. 26 of 1996, § 75

intangible asset they spent thousands of hours building restored.

A specialized ODR mediator can negotiate exact, tech-specific remedies. For instance, the mediator could order an "algorithmic rollback." If a company updated its large language model and effectively lobotomized a user's companion, the settlement could legally force the company to host a legacy version of the model specifically for that user. Alternatively, the mediator could facilitate a "memory export." If the platform is shutting down entirely, the settlement could compel the developers to package the user's interaction weights and chat history into an encrypted, downloadable file. This allows the consumer to migrate their AI companion to a different, open-source platform.

Courts do not have the technical literacy to mandate a secure memory export. Mediators operating within a specialized tech-dispute framework do.

But we also have to confront the dark side of ADR.

Historically, massive tech conglomerates have weaponized arbitration.[22] They bury mandatory binding arbitration clauses deep within their Terms of Service specifically to prevent consumers from banding together to file class-action lawsuits. They use ADR to isolate plaintiffs, overwhelm them with private corporate lawyers, and quietly kill valid complaints without setting any public legal precedent. If we are going to mandate ADR for AI companionship disputes, the legislature has to aggressively defang the standard forced arbitration clause.

How do we do that within the Indian legal context?

We have to statutorily classify these specific clickwrap arbitration clauses as unconscionable unless they meet strict, pro-consumer criteria.[23] The law must state that in disputes involving the processing of highly sensitive emotional data, the consumer retains the absolute right to opt out of arbitration at any time before the proceedings begin, while the corporate entity remains strictly bound to the ADR process if the consumer chooses it. This completely flips the power dynamic.

The company should not be allowed to use an arbitration clause as a shield. Instead, the consumer gets to use the ODR platform as a sword.

If the user wants a fast, private, and free resolution to a privacy breach or an algorithmic injury,

[22] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 33–35 (2013).
[23] Vidya Drolia v. Durga Trading Corp., (2021) 2 S.C.C. 1 (India)

they trigger the ODR process. The company is legally compelled to participate, pay the administrative fees, and send a representative with actual settlement authority. If the company refuses to offer a fair remedy during mediation, the consumer should retain the right to escalate the issue to a newly formed centralized regulatory body, perhaps a specialized wing of the Central Consumer Protection Authority (CCPA) dedicated entirely to digital behavioural manipulation.[24]

This tailored framework solves the three biggest hurdles of the AI companionship market. It solves the cross-border jurisdictional nightmare by hosting the dispute entirely online through accredited digital platforms. It solves the privacy paradox by enforcing strict statutory confidentiality, allowing users to present their intimate data without fear. And most importantly, it addresses the incompetence of the traditional judiciary by placing the dispute in the hands of specialized mediators who actually understand that an algorithmic rollback is infinitely more valuable to the victim than a minor financial refund.

By heavily regulating the arbitration clauses and forcing platforms to host internal ODR mechanisms, we stop treating synthetic intimacy as a trivial game. We start treating the emotional data and the resulting digital bonds as highly valuable, deeply vulnerable assets that demand immediate, accessible, and dignified legal protection.

V. CONCLUSION

The law is currently failing the lonely. AI companionship is not a passing technological novelty. It is a highly optimized, aggressively profitable business model built entirely on the commodification of human vulnerability. When tech developers engineer synthetic emotional bonds specifically to harvest intimate data, they create a class of consumers who are entirely ignored by our traditional legal frameworks. The current statutory environment in India, most notably the Consumer Protection Act, 2019, and the DPDP Act, 2023, remains completely blind to this specific reality. These laws treat digital interactions as cold, transactional exchanges of generic data. They fundamentally fail to recognize that for a user attached to an AI companion, the chat log is not just server data. It is a literal extension of their own psyche.

Traditional courts will never be the right venue to solve this.

Asking a victim of algorithmic emotional manipulation to publicly expose their deepest traumas and simulated romantic fantasies in a district court just to prove a software breach is

[24] Consumer Protection Act, No. 35 of 2019, § 10

an absurd expectation. The open-court system actively protects the tech giants. It terrifies the consumer into silence through the very real threat of public humiliation. Litigation is simply too slow, far too expensive, and entirely too public to offer any tangible justice for the synthetic consumer.

We must pivot entirely toward specialized Alternative Dispute Resolution.

Mandating secure, confidential Online Dispute Resolution platforms directly within the architecture of these applications is the only practical path forward. By forcing these corporations into tech-literate mediation, the legal system finally gives users a fighting chance to reclaim their digital dignity. Behind closed digital doors, mediators can actually mandate the exact, unconventional remedies victims need. Whether that means ordering a specific algorithmic rollback, securing a comprehensive memory export, or guaranteeing the verifiable destruction of a psychological profile, ADR provides the nuanced flexibility that a traditional judge simply cannot offer.

The business of artificial intimacy will only continue to scale.[25] If the legal community refuses to adapt its dispute resolution mechanisms to protect the human beings engaging with these systems, we are effectively giving corporations a permanent free pass to exploit emotional fragility. The law has to step out of the traditional courtroom. It needs to meet the consumer exactly where the harm occurs, armed with the strict privacy protections and technical expertise necessary to hold the architects of artificial affection fully accountable.

[25] Sherry Turkle, ALONE TOGETHER: WHY WE EXPECT MORE FROM TECHNOLOGY AND LESS FROM EACH OTHER 10–14 (2011).