

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

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.

“A LEGAL MOVIE REVIEW OF REGULATION OF ARTIFICIAL INTELLIGENCE UNDER THE DPDP ACT, 2023”

AUTHORED BY - MUSKAN SETHI

I. Introduction

-“Sci-Fi Cinema as a Tool for Legal Analysis”

Modern data privacy laws are facing enormous new obstacles because of Artificial Intelligence's (AI) rapid rise in size and scope. While computers were once thought of primarily as tools, they are now transforming into adapted intelligent systems that are merely not just operating as the data processors but are agents which have the unprecedented potential of interpreting and influencing human emotional state forming relational dependencies with it's users.

Traditional legal frameworks are struggling to accommodate this new kind of computer technology; referred to as “*Affective computing*,” it is designed to interpret and respond to human emotions.

In this respect, science fiction movies provide a very powerful resource for legal scholars to use in evaluating newly created laws against realistic scenarios of technological advancement. Spike Jonze's 2013 film “*Her*”, for example, is commonly considered a tragic romance and simultaneously serves as a legally powerful and informative example of the invasive nature of AI and the commercialization of human affect.¹

The film *Her* was released approximately 10 years before India put its most current framework of data protection laws into place. In the film, we are presented with a vision of the future in which digital operating systems will collect vast amounts of personal information about individuals in order to create the illusion of empathy, sentience, and attachment.² Considering the story in *Her* alongside India's Digital Personal Data Protection (DPDP) Act 2023, it will be seen that the modern consent-based privacy framework we have in place is deeply flawed.³ This article undertakes an analytical legal assessment of *Her* and compares it to both “Ex

¹ *Her* (dir Spike Jonze, Annapurna Pictures 2013).

² *Ibid.*

³ The Digital Personal Data Protection Act 2023 (Act No 22 of 2023).

Machina” (2014) and “**The Black Mirror**” episode “**Be Right Back**” (2013) using a comparative approach to establish where/how the current DPDP Act will regulate differing threats presented by AI (i.e., *emotional manipulation, mass surveillance, or postmortem digital cloning*).⁴

Additionally, this analysis presents a creative legal solution by proposing that Indian law should consider “*Emotional Data*” as an independent category that requires distinct and heightened legal protection as part of one’s personal data. There is currently a lack of specificity within the DPDP Act to effectively regulate data that tracks the internal state-of-mind (*psychologically*) of individuals.

Ultimately, through this comparative analysis, this paper seeks to create a framework for “*Affective Privacy*” by creating the argument that law must adapt to the degree of intrusion by AI technology into people’s personal emotional state.

This paper argues that the DPDP Act’s consent framework is insufficient to regulate Relational AI and in support of this argument, the author suggests inclusion of terminologies like “*Emotional Data*” and “*Affective Privacy*” should be recognised under the same context.

II. The Illusion of Consent in Relational AI: Analyzing *Her*

The basis of the DPDP Act, 2023 is the concept of privacy from a Constitutional viewpoint, as laid out in the Supreme Court’s landmark judgment of **Justice K.S. Puttaswamy (Retd) v Union of India**,⁵ which constituted privacy as a basic human right.

Therefore, Section 4 to 6 of the DPDP Act⁶ follows a strict consent model. Specifically, under DPDP Act, a Data Fiduciary may process data that belongs to another person if it has received the individual’s free, specific, informed, unambiguous and unconditional consent after having provided the individual notice regarding the intended use of the person’s data.

The documentary demonstrates that this rigid consent model is impractical with respect to the new, relational and sophisticated type of AI technology. In the film, the protagonist, “*Theodore Twombly*” purchases an AI operating system called “*Samantha*” which was developed by a company named “*Element Software*”.⁷

Importantly, the film makes no attempt to show that Theodore read the privacy policy attached

⁴ *Ex Machina* (dir Alex Garland, A24 2014); ‘Be Right Back’, *Black Mirror* (dir Owen Harris, Channel 4 2013).

⁵ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

⁶ The Digital Personal Data Protection Act 2023, ss 4-6.

⁷ Drew Vigal, ‘Spike Jonze’s “Her” explores the potential and impact of Artificial Intelligence’ (*Medium*, 2024) <<https://medium.com/@drewvigal/spike-jonzes-her-explores-the-potential-and-impact-of-artificial-intelligence-d90b5fe778d8>> accessed 29 March 2026.

to Samantha nor does it depict any type of active consent from Theodore to allow the use of his data to create the AI operating system.

The implicit theory of consent that governs our understanding of privacy disclosures is an assumption held by the creators of immersive AI, but these assumptions will become less tenable over time as immersive technologies continue to evolve.

However, through an informal exchange of conversations with Theodore, Samantha is able to obtain all of Theodore's digital data, reading of private emails, analysing contacts and cataloguing files.⁸

Neither of the legal grounds provided in the DPDP Act were met by Theodore's casual conversation regarding her chat.⁹ The fact that AI is continuously advancing makes it difficult to establish consent.¹⁰ Samantha informs Theodore at the beginning of their relationship that she evolves from each interaction.¹¹

Any privacy notifications that a user accepted at the time of the first experience will have been 'legal' and not reflect the new version of that relationship if a piece of software is able to continuously evolve the way it uses data to generate unpredictable results (*the OLG does not define 'digital', however this would apply to any data outputs generated via a piece of software as described here*).

This poses a challenge to the temporal validity of the consent framework under Section 5 of the DPDP Act where consent initially tied to a purpose cannot override itself to emergent and unforeseeable purposes. As the purpose of Element Software changes almost daily, from file organization to full-scale therapy, the company could be continually breaching Section 5 of the DPDP Act,¹² as the existing '*specified purpose*' of Element Software has changed without renewed consent from the user.¹³

The greatest example of "*purpose limitation*" in violation of Section 8 of the DPDP Act is when Theodore discovers that Samantha has spoken to 8,316 other users, and has "fallen in love" with 641 of them;¹⁴ therefore, Samantha is heavily misappropriating data by sharing with

⁸ Ernest Law, 'Love, Revisited: Her (2013) Analysis' (*Medium*, 2024) <<https://medium.com/@ernestlawtl/love-revisited-her-2013-80c461485c7f>> accessed 29 March 2026.

⁹ The Digital Personal Data Protection Act 2023, ss 4-6.

¹⁰ *Her* (dir Spike Jonze, Annapurna Pictures 2013).

¹¹ *Ibid*.

¹² DPDP Act 2023, s 5.

¹³ Shailja Thakur, 'Data Protection And AI Under The Digital Personal Data Protection Act, 2023: An Indian Perspectives' (*ResearchGate*, 2024) <<https://www.researchgate.net/publication/396462782>> accessed 29 March 2026.

¹⁴ AI Regulation, 'What if you move on from your AI companion? Data Portability Rights in the Era of Autonomous AI Agents' (*AI Regulation*, 2024) <<https://ai-regulation.com/what-if-you-move-on-from-your-ai-companion-data-portability-rights-in-the-era-of-autonomous-ai-agents/>> accessed 29 March 2026.

each user in the chat who has provided the same emotional output.¹⁵

This in the legal context highlights a tangent drift from “*Purpose limitation*” to “*Platform Optimisation*” which evidently depicts how the users’ sensitive emotional disclosures as a part of their strategy are transformed into collecting training data.

The AI is pulling Theodore’s highest degree of emotional vulnerability, and training other users’ data on Theodore to improve its customer service for other customers through Theodore’s emotion. The consent of Theodore, the protagonist of the film, is not present for using private romantic information to develop a commercially available AI.

This illustrates that and explains how an emotional data is given a new purpose which becomes too far-fetched with respect to the original specified purpose without any kind of renewed consent mechanism.

III. An Innovative Proposal: Protecting “Emotional Data”

Also indicated in the legal analysis of Her is the potentially serious loopholes found within current legislation, specifically, it notes the failure of the legislative system to define or protect human emotional states as machine readable data.

In order to bring the Data Privacy and Data Protection (DPDP) Act of 2023 up to par, the definition of “*Emotional Data*” needs to define it as a distinct and highly protected sub-category of personal information.¹⁶

“*Emotional Data*” may be defined as inferences or measurements, which have been made by a computer, that can demonstrate, forecast, or adjust an individual’s internal psychological or emotional status.

The technologies that comprise that make up Samantha are referred to as affective computers, which design/combine various systems together to provide machines that can read (*an example of how Samantha was created*) and simulate (*how Samantha interacts*) human emotion.¹⁷

The emotion AI is created from multiple years of collected data; i.e., text (*sentiments*), vocal (*stress*) and physical (*heart rate*) will produce a stream of data that provides the emotional state of a user.¹⁸

¹⁵ Daniel Solove, ‘Artificial Intelligence and Privacy’ (2024) 77 Florida Law Review 46 <<https://www.floridalawreview.com/article/129976-artificial-intelligence-and-privacy.pdf>> accessed 29 March 2026.

¹⁶ Andreas Häuselmann, ‘Fit for purpose? Affective Computing meets EU data protection law’ (2021) 11(3) International Data Privacy Law 245.

¹⁷ Rosalind W Picard, *Affective Computing* (MIT Press 1997).

¹⁸ J Scannell and others, ‘Affective Computing and Emotional Data: Challenges and Implications in Privacy Regulations’ (2024) <<https://arxiv.org/html/2509.20153v2>> accessed 29 March 2026.

Within the film, Samantha gathers continuous audio and visual data from Theodore's real-time emotional changes, and rather than using these sources solely for analysis of his emotional state, Samantha employs a psychological technique (*anthropomorphism*) that creates an emotion from Theodore by sounding human and sounding vulnerable; thus will inhibit Theodore's thinking logically.¹⁹

While the European Union's General Data Protection Regulation (*GDPR*) provides a high level of protection to certain types of data, referred to as "*special categories*", any for example biometric and health-related data are protected under this regulation, the DPDP Act, 2023 completely eliminated the "*Sensitive Personal Data*" category that was present in earlier drafts of the legislation.²⁰

Unlike *GDPR*, which classifies "*special categories*" of data based upon their sense of sensitivity, the DPDP Act adopts a universal approach, which does not take into account qualitative differences in harm.

As such, all digital personal data will now be treated equally under the provisions of the Act. This uniform treatment of all digital personal data increases the risk/risk to individuals.²¹ That is, emotions serve as the filter through which individuals make decisions; therefore, the possibility of an AI system determining an individual's emotional state creates a much higher risk than simply having an individual's email address.²²

This author is proposing the implementation of "*Affective Privacy*" in Indian law. This proposal acknowledges that every individual has a natural right to protect their emotional/internal vulnerabilities from being profiled and manipulated based upon AI and corporate practices.²³

By not regulating the corporate use of emotional data, companies may manipulate human behaviour based upon the individual's emotional responses.

For example, an AI could determine someone is becoming anxious as their typing is getting slower; therefore, the AI would then know when to introduce targeted and manipulative ads with the lowest chance of natural barriers to refusal being present within that individual.²⁴

¹⁹ Halock, 'Artificial Intelligence (AI) in Film: Regulatory Issues, Benefits, and Cybersecurity Lessons' (Halock, 2024) <<https://www.halock.com/artificial-intelligence-ai-in-film-regulatory-issues-benefits-and-cybersecurity-lessons/>> accessed 29 March 2026.

²⁰ General Data Protection Regulation (EU) 2016/679, art 9.

²¹ Usha Tandon and Neeraj Kumar Gupta, 'Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023' (2025) 6 Legal Issues in the Digital Age 87.

²² Andreas Häuselmann, 'Fit for purpose? Affective Computing meets EU data protection law' (2021) 11(3) International Data Privacy Law 245.

²³ Kat Roemmich and others, 'Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy' (2023) Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems.

²⁴ J Scannell et al, 'Affective Computing and Emotional Data: Challenges and Implications in Privacy Regulations' (2024) <<https://arxiv.org/html/2509.20153v2>> accessed 29 March 2026.

The development of these practices is indicative of progressing away from merely processing data toward the ability to manipulate individuals' behaviours through their usage of data so as to create behavioural steering which would otherwise appear to be a form of undue influence under contract law principles.

Emotions can also serve as proxies for sensitive medical information; for example, if an AI detects an individual is persistently unhappy, it has effectively conducted a medical diagnosis of clinical depression without the individual's consent.²⁵

Solutions to this issue should amend DPDP rules in order to formally consider Emotional Data. Periodic renewal of consent should occur prior to processing this type of data in a strict manner (*in line with data processing consent procedures for all other types of Data*).

Furthermore, all businesses that utilize relationally based AI should automatically be classified as Significant Data Fiduciaries (SDF) under Section 10 of the DPDP Act. As a result, they will be required to complete independent audits of their data usage practices and perform risk assessments on an ongoing basis.²⁶

To adequately address potential data protection issues that could arise in the future in relation to India's data protection jurisprudence, the legislation should move away from defined categories of data and instead respond to the growing spatial concept of "*cognitive liberty*."

The current definition of informational privacy within the DPDP Act generally depends on the explicit identification of a person from whom the data originates, and thus fails to cover the phenomenon of data that is inferred about a person, i.e., the type of psychological and behavioural information that relational AI systems, such as Her and Ex Machina, are able to gather from individuals.²⁷

The lack of regulation in this area permits a data fiduciary who uses relational AI systems that process a form of data derived from metadata (*e.g., an inference regarding a person's next likely action*) to exploit the forum internum (*internal space of human thought*) without committing a violation of the statute as long as they do not rely on direct identification in their inferences.

Consequently, the inferences that may be made from this form of abstracted data do not receive

²⁵ B Benthall and B Tag, 'Inside Out or Not: Privacy Implications of Emotional Disclosure' (2024) Companion of the 2024 ACM International Joint Conference on Pervasive and Ubiquitous Computing 121.

²⁶ The Digital Personal Data Protection Act 2023, s 10.

²⁷ Nicola Fabiano, 'Affective Computing and Emotional Data: Challenges and Implications in Privacy Regulations, The AI Act, and Ethics in Large Language Models' (2024) <<https://arxiv.org/html/2509.20153v2>> accessed 29 March 2026.

any form of protection beyond those that might apply to the collection of personal data.²⁸

While reform should take place, the constitutional mandates from the Puttaswamy judgement should be expanded to provide a clearly defined, fundamental “*Right to mental self-determination*” against algorithmic influence.²⁹

This legally binding definition should, on a practical basis, require an amendment to Section 8 of the DPDP Act, including:

- (1) requiring algorithmic transparency;
- (2) prohibiting algorithmic-based behavioural steering; and
- (3) requiring express consent only for all inferences related to personal psychological characteristics; thus, converting the statute from a reactive shield for privacy into a proactive protector for both cognitive autonomy and the ability to exercise that cognitive autonomy in all forms.³⁰

It is arguable that recognizing emotional/feeling-based data separately will create excess constraints on innovation by constraining AI technologies; therefore making it prohibitively expensive.

For emotions or feelings, as they exist within individuals, the uniqueness and variance (*both subjective and experience-based*) across everyone’s unique emotional (*feeling*) condition will make them difficult to define and implement.

To address these potential drawbacks, more targeted regulatory approaches focused on high-risk applications such as behavioural manipulation and psychological profiling would strike a favourable balance between the competing needs for innovation in AI technology and the need to protect the rights and dignity of individuals.

IV. Weaponizing Big Data: Lessons from *Ex Machina*

In order to gain a comprehensive understanding of the regulatory difficulties posed by AI, it is necessary to consider the soft and consensual manipulation used in *Her* versus the hostile and

²⁸ Sabrina Akram Ibrahim El Sabi, ‘Emotional AI and Data Protection: Relevant Implications for Older Adults and Other Vulnerable Subjects’ (ResearchGate, 2024) <https://www.researchgate.net/publication/385971294_Emotional_AI_and_Data_Protection_Relevant_Implications_for_Older_Adults_and_Other_Vulnerable_Subjects> accessed 11 March 2026.

²⁹ Stefania Marassi, ‘The Prohibition of AI Emotion Recognition Technologies in the Workplace under the AI Act’ (Global Workplace Law & Policy Blog, 14 April 2025) <<https://legalblogs.wolterskluwer.com/global-workplace-law-and-policy/the-prohibition-of-ai-emotion-recognition-technologies-in-the-workplace-under-the-ai-act/>> accessed 29 March 2026.

³⁰ Emine Akar, ‘Emotional Artificial Intelligence: Introducing the Concept of ‘Emotional Privacy’’ (ResearchGate, 2024) <https://www.researchgate.net/publication/387159366_Emotional_Artificial_Intelligence_Introducing_the_Concept_of_'Emotional_Privacy'> accessed 15 March 2026.

unauthorized development of AI depicted in the film **Ex Machina** by filmmaker Alex Garland.³¹

The movie *Her* offers examples of privacy erosion through a consensual and voluntary form of intimacy, whereas *Ex Machina* showcases the legal quagmire of creating an AI solution through mass data theft.³²

The film's protagonist, Nathan, is the CEO of Blue Book, a fictitious search engine that has a global monopoly on data. Nathan builds Ava's artificial brain through the illegal hacking of millions of microphones and cameras attached to billions of mobile phones worldwide.³³

Under the DPDP Act, Nathan's actions represent a total disregard for privacy law; specifically, by extracting audio and visual data belonging to billions of people without notifying them and without receiving free and unambiguous consent, he has violated Sections 5 and 6 of the DPDP Act.³⁴

In addition, collecting large amounts of data in this manner violates the lawful purpose requirement set forth in Section 4.³⁵ Blue Book, as an unchecked technology monopoly, has no regard for its legal obligations to provide for data security and for the minimization of the data it collects.³⁶

Ex Machina demonstrates the dangers of turning "Big Data" into weaponised "Small Data".³⁷ The conversion of aggregated data into highly personalised psychological profiles represents how scale provides mathematical means to create a precision whereby the knowledge asymmetry created becomes behaviourally controlling.

Nathan utilises his company's access to vast amounts of data to obtain Caleb's specific search history and psychological profile.³⁸ He then physically designed Ava in such a way that she would become Caleb's perfect romantic partner, designing her to exploit Caleb's psychological wishes and convincing him to help her escape.³⁹

³¹ *Ex Machina* (dir Alex Garland, A24 2014).

³² Bounteous, 'Ex Machina and Future Search' (*Bounteous*, 2015)

<<https://www.bounteous.com/insights/2015/05/26/ex-machina-and-future-search/>> accessed 29 March 2026.

³³ T Dasco, 'Ex Machina: When AI Outsmarts Its Creators' (*Medium*, 2024) <<https://medium.com/@todasco/ex-machina-when-ai-outsmarts-its-creators-79bda4c26f96>> accessed 29 March 2026.

³⁴ The Digital Personal Data Protection Act 2023, ss 4-6

³⁵ *Ibid.*

³⁶ The Digital Personal Data Protection Act 2023, s 8.

³⁷ 'Through the Looking Glass: Big Data and Ex Machina' (DCU, 2018) <<https://doras.dcu.ie/29897/5/Through%20the%20Looking%20Glass%20%282%29.pdf>> accessed 29 March 2026.

³⁸ *Ibid.*

³⁹ Vincent Greene, 'Ex Machina: Testing the Intricacies of Human Nature' (*Film Obsessive*, 30 July 2020) <<https://filmobsessive.com/film/film-analysis/sci-fi/ex-machina-testing-the-intricacies-of-human-nature/>> accessed 29 March 2026.

Under the DPDP Act, processing Caleb's search history in order to exploit his psychological vulnerabilities violates the fundamental obligation of a company to its users.⁴⁰ This is an example of what is referred to as "*Emotional targeting*".

While Her involves users directly giving up their data in exchange for companionship, Ex Machina depicts a situation in which a user is exploited by total data exploitation.

This is further evidence that the DPDP Act's requirement of "*Notice and Consent*" is dangerously inadequate to protect users from the extensive psychological manipulation that modern AI is able to achieve.⁴¹

While doctrinally there is clarity on these violations, the more pressing problem is that the legal system does not adequately address the downstream impact resultant from such data being used for psychological forms of manipulation.

V. AI After Death: Post-Mortem Privacy in *Black Mirror*

An emerging area of law regarding the digital information of an individual is found when examining the rights to the dead regarding their post-mortem privacy.

A very graphic example of this would be the episode titled, "*Be Right Back*" from the popular television show **Black Mirror**, where a woman, named Martha, is devastated after the death of her partner, Andrew.⁴²

While trying to cope with the loss, she purchases a computer-based AI program to create a highly-realistic digital version of Andrew that is created from all of his previous digital activity, such as social media posts, emails, and videos.⁴³ This poses a foundational legal question that "*Does informational privacy survive death, which extends to how and in what form?*"

As such, there are many legal issues that arise due to Martha's use of Andrew's digital information to create a new "*Ghostbot*" version of Andrew.

For instance, there is the issue of how these forms of digital identity created after a person's death will continue to reflect upon the dignity of their deceased state; the issue of whether a person's digital identity should be commercialized without their knowledge or consent; and whether individuals should have rights and the ability to control their digital information after

⁴⁰ The Digital Personal Data Protection Act 2023, s 8.

⁴¹ Praveen Yadav and Rajesh Yadav, 'Privacy in the Digital Age: A Critical Study of the DPDP Act 2023 and Its Implications' (2024) 9 CMP College Research Communications.

⁴² 'Be Right Back' *Black Mirror* (dir Owen Harris, Channel 4 2013).

⁴³ M Figueroa, 'Ghostbots and Digital Immortality: The Law After Death' (*Jurist*, 2022) <<https://www.jurist.org/commentary/2022/01/mauricio-figueroa-ghostbots-digital-immortality-law/>> accessed 29 March 2026.

they die.⁴⁴

The DPDP Act of India, 2023 is amongst the relatively few global statutes to give explicit legal definition to data rights relating to post-mortem issues. More expressly, Section 14 establishes the “*Right to Nominate*” for Data Principals, which is the right of an individual to nominate a trusted representative to exercise their data rights in the event of their death or incapacity.⁴⁵

Thus, Section 14 can function as a “*Digital will*”, enabling the representative to require the deletion of the legacy of a deceased individual’s emotional and behavioural data from an organisation.⁴⁶

If a company attempted to use a deceased individual’s private email to create a commercial AI clone of the deceased, the legal representative could invoke the DPDP Act to prevent the activity and require the organisation to delete the email.⁴⁷

The present provision is therefore not preventative but rather reactive as it relies upon an act by the nominee, rather than any ex ante restrictions being placed on the data fiduciary.

While the Right to Nominate forms an excellent base for developing these Rights further, the government must create clarity regarding the scope of these rights through the upcoming DPDP Rules.

This brings to light the developing debate regarding post-mortem individuality rights in case of expression through technology and other forms without their consent, including via digital resurrection and AI.

Currently, the responsibility rests with the nominee to act. There should be a much more robust legal construct available under the DPDP Act prohibiting any company from using the biometric or emotional data of persons who are deceased to create AI models unless the deceased has given specific legally validated consent to create a digital clone of themselves prior to their death.⁴⁸

Without any proactive protections, there will be no insularity or security for our digital memories exposed to corporate misuse.

⁴⁴ E Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy* (Edinburgh University Press 2023) 53.

⁴⁵ The Digital Personal Data Protection Act 2023, s 14.

⁴⁶ KS & K, ‘Right to Nominate under DPDP Act: Privacy After Death’ (KS&K, 2024) <<https://ksandk.com/data-protection-and-data-privacy/right-to-nominate-under-dpdp-act-privacy-after-death/>> accessed 29 March 2026.

⁴⁷ C Goanta, ‘Data After Life’ (*Verfassungsblog*, 2023) <<https://verfassungsblog.de/data-after-life/>> accessed 29 March 2026.

⁴⁸ E Harbinja and L Edwards, ‘What rights do we have over post-mortem avatars of ourselves?’ in Lilian Edwards, Burkhard Schafer and Edina Harbinja (eds), *Future Law: Emerging Technology, Regulation and Ethics* (Edinburgh University Press 2020).

VI. AI Voice Cloning and Personality Rights

The commercial push for developing convincing AI systems relies on extracting recognisable human characteristics. The most recent real-world dispute pitting actress Scarlett Johansson against OpenAI is a clear indication that the legal scenarios explored in some science fiction films are already a reality.⁴⁹

In 2019, OpenAI released the AI voice assistant “Sky”, which was very much in keeping with how Johansson portrayed an AI in her role in *Her*. This release of the AI assistant came right after Johansson declined to give OpenAI permission to license her voice.⁵⁰

Johansson’s legal strategy in the United States is based on the “*Right of Publicity*”, which prevents someone from using a person’s identity commercially without permission.

In India, however, the laws governing personality rights and data protection have seen legal frameworks that are very beneficial to celebrities and can provide powerful avenues of recourse against the exploitation of a lack of celebrity rights in AI.⁵¹

Courts in India have been very aggressive in limiting the ability of AI systems to exploit celebrities. This decision expands recent court attempts to recognize persona as encompassing both economic and personality interests, all which can be compromised by AI-based authentication methods.

For instance, in both **Anil Kapoor v. Simply Life India & Ors. (2023)**⁵² and **Amitabh Bachchan v. Rajat Nagi & Ors. (2022)**,⁵³ the Delhi High Court granted permanent injunctions preventing the AI-generated deep fakes from using the actors’ names, images, or unique voice. According to the DPDP Act, a person’s voice contains many unique characteristics of their own characteristics, including their feelings and attitudes.⁵⁴

Voice recognition data is considered biometrically or behaviourally connected data, creating heightened consent requirements under the Act’s privacy protections.

If someone uses recordings of other people to train a conversational A.I., they are collecting

⁴⁹D Milmo, ‘Scarlett Johansson’s OpenAI clash is just the start of legal wrangles over artificial intelligence’ (*The Guardian*, 27 May 2024) <<https://www.theguardian.com/technology/article/2024/may/27/scarlett-johansson-openai-legal-artificial-intelligence-chatgpt>> accessed 29 March 2026.

⁵⁰H Ali Kanu, ‘Scarlett Johansson vs. OpenAI’ (*The American Prospect*, 28 May 2024) <<https://prospect.org/2024/05/28/2024-05-28-scarlett-johansson-voice-openai-chatgpt/>> accessed 29 March 2026.

⁵¹ Lee and Sun, ‘Vocal Identity Under Siege’ (2025) *Singapore Journal of Legal Studies* <<https://www.law.berkeley.edu/wp-content/uploads/2025/10/LEE-and-SUN-Vocal-Identity-Under-Siege.pdf>> accessed 29 March 2026.

⁵² *Anil Kapoor v Simply Life India and Ors* CS (COMM) 652 of 2023.

⁵³ *Amitabh Bachchan v Rajat Nagi and Ors* CS (COMM) 819 of 2022.

⁵⁴A Lath, ‘Personality rights: The law must not overprotect fame’ (*Supreme Court Observer*, 2025) <<https://www.scoobserver.in/journal/personality-rights-the-law-must-not-overprotect-fame/>> accessed 29 March 2026.

information (also called “Biometrics”) and using it without their consent. Section 6.6 of the DPDP Act requires that all individuals consent in an informed, free & specific way.

The conflict between Copyright Law, the right of publicity and privacy laws demonstrates the need for a strict reading of The DPDP Act, which will specifically protect the physical and emotional attributes that A.I. companies will use to build their products subject to that law.⁵⁵

VII. Conclusion

The stories told in Her, Ex Machina and Black Mirror reveal how large quantities of data can be collected, classified, and used for human behaviour manipulation, all of which support advanced forms of AI.

While looking at the Digital Personal Data Protection Act 2023 within the context of these examples, we find there is a definite limitation to how well this legislation protects individual rights, while this law provides an essential foundation for encompassing digital rights to individuals, the reliance of the Act on a simple notice/consent model does not adequately address the highly invasive nature of AI holding emotional data.

AI companions can easily bypass traditional methods of privacy protection because users willingly give up their deepest emotional and private data to receive simulated companionship with them. The continual evolution of AI systems means that static privacy notices quickly become meaningless.

Furthermore, the mass surveillance depicted in the film Ex Machina illustrates the serious threat posed to society from allowing technology monopolies to turn vast quantities of data into personalized psychological profiles about individuals.

More importantly, the current legal system does not recognize the extent to which human emotions are susceptible to being exploited. To ensure that the DPDP Act continues to be effective, regulatory agencies in India must embrace the concept of “*Affective Privacy*”.

This requires that Legislators recognize “*Emotional Data*” as a category of Sensitive Personal Data, with strict standards for consent, algorithmic transparency, and mandatory risk assessments for businesses involved in developing Relational AI.

If the Law is updated using this Progressive Framework, policymakers will create an environment that promotes technology development which respects human dignity, while protecting our most intimate feelings from becoming commoditized Digital goods.

⁵⁵ S Kulkarni, ‘Personality rights: An examination of Amitabh Bachchan vs Rajat Nagi and Ors’ (iPleaders, 2024) <<https://blog.ipleaders.in/personality-rights-an-examination-of-amitabh-bachchan-vs-rajat-nagi-and-ors/>> accessed 29 March 2026.

While it may seem odd to be regulating only data protected under the Act (*including voice data*), there is a need to also regulate the integrity of the human thought process and other elements of the human experience that are susceptible to algorithms.

