LICENSING THE SELF: REINING IN CONTRACTUAL EXPLOITATION OF DIGITAL PERSONA IN INDIA'S PLATFORM AND CREATOR ECONOMY

Deepansh Jain, LLM, Christ (Deemed to be University), Delhi NCR

ABSTRACT

This article argues that India's current legal framework for protecting personality and privacy is not equipped to deal with the ways digital platforms and other institutions now capture and commercially exploit digital persona, including elements like a person's face or voice and even their avatars, through standard-form contracts. While courts have increasingly recognised personality rights as an aspect of Article 21 dignity and privacy, and data-protection law acknowledges harms such as identity theft and reputational damage, these frameworks operate largely ex post and focus on discrete instances of misuse. In practice, however, the deeper risk emerges earlier, as standard-form agreements often grant "perpetual, worldwide, royalty-free" rights over user-generated content and performances. Once generative AI enters the picture, these clauses effectively become the legal basis for training models on a person's likeness or voice, enabling the creation of synthetic doubles that can act independently, even long after the original relationship has ended.

The article traces this contractual terrain across platform terms and media and entertainment agreements, with brand–influencer deals forming a distinct extension of the same logic. It shows how current drafting folds different interests into one expansive licence. Control over content is treated as interchangeable with control over data processing. From there, it stretches further to cover persona replication, even though that raises a different set of concerns. The discussion then turns to Indian law. It identifies gaps in personality-rights jurisprudence and reads them alongside constitutional privacy doctrine. Data-protection law is brought in more cautiously, mainly to show how bundled consent operates when identity is exploited through AI systems. Comparative material is used with restraint. The United States offers insight through publicity rights. The European Union provides a different angle, particularly on biometric data and emerging AI regulation. These are not presented as models to copy. Instead, the article isolates specific techniques, stricter consent standards in some contexts, clearer disclosure around synthetic media in others, and limited protections for

performers. The emphasis remains on adapting these ideas to India's constitutional framework and its market conditions.

The article advances the idea of identity-centric contracting, urging that agreements covering faces, voices, and avatars should be structured with clear persona clauses, revocable consent for AI training and synthetic uses, purpose- and time-bound licences, fair remuneration for autonomous avatars or cloned voices, and non-waivable dignity safeguards against degrading or deceptive exploitation. These principles are illustrated through model clauses and sector-specific scenarios spanning short-video platforms, influencer campaigns, and performer or voice-actor arrangements. Regulatory levers are identified in intermediary rules, data-protection enforcement, advertising self-regulation, and labour or sectoral norms to embed identity-centric standards into law. The conclusion warns that without recalibration, Indian contracting risks locking individuals into perpetual licences over their own technologically manufactured doubles.

Keywords: Digital persona, Platform contracts, Personality rights, Creator economy, Data protection, Generative artificial intelligence, Identity-centric contracting.

1. Introduction: Contract as the New Site of Personality Capture

In contemporary India, the most significant threats to personality rights are no longer confined to spectacular deepfake scandals or isolated instances of unauthorised endorsements. They are increasingly embedded, quietly and systematically, in the standard form contracts that govern participation in the platform and creator economy. Employment agreements and influencer contracts, together with click-wrap terms for social media and AI tools, now operate as invisible machinery through which identity is transformed into licensable assets.[1] These instruments were drafted for an era in which platforms merely hosted or distributed content. In the age of generative artificial intelligence, they have become the legal foundation for training models on human likeness and synthesising "digital doubles" that can continue to speak and endorse, while also performing long after the original person has logged out or moved on.[2]

This shift from episodic misuse to structural contractual capture raises a fundamental normative question: should Indian law continue to treat facial images and voice recordings, along with

[1] AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025.
[2] Mark Fenwick and Paul Jurcys, "Digital Twins Demand a New Social Contract", TechPolicy.Press, 17 November 2025.

stylised on-screen performances, as just another category of "content" or "data," subject to broad perpetual licences in boilerplate agreements, or should it recognise them as elements of a digital persona that demand a higher standard of consent and control?[3] The answer cannot be left entirely to unequal bargaining between global platforms and individual users, or between production houses and gig-based creators. Indian courts have begun to recognise personality rights as an aspect of the right to privacy and dignity under Article 21 of the Constitution, and have restrained unauthorised commercial exploitation of name, image, or voice in several recent cases.[4] At the same time, India's data-protection framework formally acknowledges identity theft and reputational injury as cognisable harms.[5] Yet these developments have not meaningfully constrained the way contracts silently convert identity into raw material for AI training and synthetic endorsements.

The concern is not merely theoretical. Globally, commentators have shown how website terms and click-wrap agreements are being used to authorise the scraping and reuse of user content, including images alongside text, for training large-scale AI models, often without any realistic possibility of negotiation or opt-out.[6] In parallel, scholarship on "data as likeness" has argued that biometric and behavioural traces can function as a proxy for persona, enabling generative systems to create outputs that closely resemble a person's face or voice, or even their style, without overt reliance on traditional likeness markers.[7] In India, personality-rights analysis in the AI context has so far focused on obvious misuses such as deepfake pornography and deceptive endorsements, together with cloning of celebrity performers. These discussions highlight doctrinal gaps and call for stronger consent-based licensing regimes.[8] What remains under-examined is the more mundane layer at which creators and workers, through standard-form contracts, sign away prospective control over AI-mediated replication of their own persona as a condition of access to work or visibility.

This article proceeds from the premise that such developments cannot be adequately addressed by relying on ex post remedies alone. Doctrines of privacy and defamation, along with passing

[3] Zahr Said Takhshid, "Data as Likeness", 112 Georgetown Law Journal (forthcoming 2024).
[4] Amitabh Bachchan v. Rajat Nagi, 2022 (6) HCC (Del) 641 (Del HC); Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Del. HC); R. Rajagopal v. State of T.N., (1994) 6 SCC 632 (SC) (deriving a right to control the commercial use of identity from Article 21).
[5] Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 2(1)(q) (India).
[6] "AI Training Models and Website Terms of Use", Chip Law Group, 18 September 2023.
[7] Zahr Said Takhshid, "Data as Likeness", 112 Georgetown Law Journal (forthcoming 2024).
[8] "Personality Rights & AI Cloning: Legal Gaps in India", Khurana & Khurana, 8 September 2025; "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).

off, unjust enrichment, and statutory tools in information technology and data-protection law, were not designed to interrogate or restructure the contractual mechanisms through which identity is commodified on a mass scale.[9] If Indian law is to prevent the normalisation of "personality capture by contract," it must move beyond case-by-case litigation and articulate a framework that treats dealings in digital persona as a special category, particularly where contracts purport to authorise AI training, cloning, or autonomous reuse of a person's face or voice.

The discussion that follows is organised in four broad moves. The next section maps the contractual terrain of Indian platforms, employers, and influencer arrangements, showing how clauses drafted for content and data now extend to digital persona with little doctrinal scrutiny. Subsequent sections examine the limits of existing personality-rights, privacy, and data-protection frameworks when confronted with bundled consent to AI-driven replication, and draw targeted lessons from foreign publicity and data regimes that grapple with biometric exploitation and synthetic identity.[10] Building on this, the article then sets out the core principles of "identity-centric contracting" and identifies specific regulatory levers in intermediary guidelines, data-protection implementation, advertising standards, and labour regulation through which these principles could be embedded into Indian law. In closing, the article argues that, unless contract and regulation are consciously reshaped, Indian creators, workers, and users will find themselves legally bound to compete not only in markets or feeds but also against their own technologically manufactured doubles.

2. Mapping the Contractual Terrain: How Indian Platforms and Employers Capture Identity

The contractual ecosystem that underpins India's platform and creator economy was largely designed for an earlier internet, where the central legal object was "content" and the primary risk was unauthorised copying or redistribution. Standard-form agreements still reflect that mindset. They speak of "user-generated content," "materials," and "data" in broad, undifferentiated terms, and treat all such inputs as licensable on a perpetual, worldwide,

[9] AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025; "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).

[10] Zubair Abbasi, "Rights Violations and Regulatory Gaps Arising from the Expansion of AI-Mediated Romance and Deepfake Relationships: A Legal and Corruption-Risk Analysis of AI Persona-Based Emotional Relationships", 13 Journal of Law & Emerging Technologies (2025); Zahr Said Takhshid, "Data as Likeness", 112 Georgetown Law Journal (forthcoming 2024).

royalty-free basis. In a generative AI environment, however, this drafting style has a very different effect. When contracts fail to distinguish between an ordinary photo and a biometric template, or between a text post and a high-fidelity voice recording, they effectively allow platforms, employers, and brands to treat an individual's likeness or voice as raw material for AI training and synthetic persona creation.

2.1 Platform Terms of Service and Click-Wrap Licences

Most major digital platforms use non-negotiable terms of service under which users grant expansive licences over everything they upload. These licences typically authorise the platform to "host, store, reproduce, modify, adapt, publish, create derivative works from, and communicate" user content, often coupled with a right to sublicense such uses to third parties. While originally justified as necessary to display content across devices and enable sharing, the same clauses now serve as the contractual basis for using images, audio, or video in training proprietary AI systems. Scholars have noted that many websites and apps explicitly reserve the right to "use content to improve services," a formulation that increasingly encompasses model training and the generation of new outputs that need not be tied to the original user's account or intentions.[11]

In this setting, the user's face or voice is subsumed within a general category of "content," even though they carry far greater potential for personality replication than, for instance, a text comment or a landscape photograph. Because the licence is granted at the point of sign-up through a click-wrap interface, users have little realistic opportunity to distinguish between consenting to basic hosting and consenting to the creation of autonomous digital doubles. Platforms can point to the literal breadth of the licence as a defence against later personality-rights claims, arguing that the user contractually authorised such uses. This creates a structural skew: while data-protection and consumer-protection norms demand clarity and fairness in consent, the underlying private contracts blur the line between necessary technical uses and transformative AI-driven exploitation of digital persona.

2.2 Employment and Engagement Contracts in Media and Entertainment

A similar pattern appears in employment and engagement contracts used in Indian media,

[11] "AI Training Models and Website Terms of Use", Chip Law Group, 18 September 2023.

entertainment, and advertising sectors, where artists and technicians often sign agreements that assign "all rights" in their performances to producers or studios. Traditionally, such clauses were understood as transferring copyright and neighbouring rights in fixed recordings, allowing producers to exploit films, soundtracks, or commercials across platforms. With the advent of AI, however, the same assignments can be read to authorise training and deployment of synthetic versions of the worker's performance style, facial mannerisms, or vocal timbre.

Voice actors, for instance, may sign standard studio contracts that treat their recordings as works made in the course of employment, with all rights assigned in perpetuity for "all media now known or hereafter devised." As generative text-to-speech systems become more sophisticated, producers can feed those recordings into models capable of generating new lines in the actor's voice without additional sessions or fees. Legal commentary on performance and publicity rights has warned that such practices risk hollowing out the economic value of performers' identities, turning them into a one-time input for an indefinitely exploitable synthetic persona.[12] Yet absent explicit contractual language distinguishing between conventional reuse and AI-mediated cloning, performers are left to argue that the original bargain did not contemplate such technologically enabled substitution.

The same dynamic affects on-screen performers and models. Talent agreements for advertisements and web content often grant brands the right to reuse footage, stills, or likeness "in all media" for extended periods. In an AI context, this can cover not only the re-editing of existing footage but also the generation of new composites in which a model's face is merged with other bodies, settings, or scripts. Without clear temporal and functional limits, a single day's shoot can underwrite years of synthetic endorsements, with no additional consent or negotiation once AI tools are integrated into the production pipeline.

2.3 Influencer and Creator Agreements

Influencers and digital creators occupy a hybrid position between platform users and contracted talent. They upload content under general platform terms, but many also sign separate agreements with brands, talent agencies, or multi-channel networks. These contracts typically contain broad publicity and IP clauses, granting the counterparty the right to use the creator's "name, image, likeness, biographical information, and content" in connection with campaigns.

[12] "Expert Take: Publicity, Privacy and Performance Rights", Economic Times – Legal, 9 November 2025.

In an AI-enabled ecosystem, such language can be invoked to justify the creation of branded avatars modelled on the creator's appearance or voice, or to run synthetic variations of sponsored posts without the creator's ongoing involvement.

Recent analyses of influencer contracts in the AI age caution that many creators, especially smaller ones, are unlikely to have legal advice or bargaining power when signing such forms, and may not appreciate that a licence to "adapt and create derivative works" could extend to training generative models on their persona.[13] The danger is that the creator's digital identity becomes partially decoupled from their control: their avatar can appear in campaigns they did not script, at times and on platforms they do not manage, and potentially even after the underlying relationship has ended. Yet because the underlying contracts are framed as ordinary commercial agreements rather than as dealings in personality rights, disputes may be litigated as straightforward matters of contractual interpretation rather than as violations of a protected identity interest.

2.4 The Blurring of Data, Content, and Identity

Across these contracts platform terms of service, employment and engagement agreements, and influencer deals a common pattern emerges. The law's traditional categories of "content," "data," and "work" are used to capture inputs that now function, in practice, as components of digital persona. Doctrinally, an image can be both personal data and copyrighted work; a recording can be both a performance and a biometric template; a video can be both a creative output and a training example. Without explicit safeguards, contract drafters can treat all of these elements as fungible objects of licence or assignment, even though their downstream uses diverge sharply once generative AI is introduced.

This blurring is particularly acute in India, where the creator and gig economies intersect with high levels of informality and power imbalance. Workers and small creators may feel compelled to accept standard terms to access opportunities, with little scope to isolate and negotiate persona-related clauses. In that environment, the interplay between contract and technology can gradually normalise the idea that faces or voices are available for perpetual AI-mediated reuse unless a person has the knowledge and leverage to carve out exceptions. The next sections argue that existing personality-rights and privacy doctrines, while valuable,

[13] "Personality Rights & AI Cloning: Legal Gaps in India", Khurana & Khurana, 8 September 2025.

do not directly confront this structural problem, and that Indian law needs a more explicit identity-centric approach to contracting in order to realign private agreements with constitutional commitments to dignity and autonomy.

3. Personality Rights, Privacy, and Data Protection: Promise and Blind Spots

Indian law has begun to assemble a toolkit for protecting personality and identity in the digital environment, but that toolkit was not designed with contractual, AI-driven exploitation of persona in mind. The resulting framework offers important ex post remedies against egregious misuse of name, image, or voice, yet it remains poorly aligned with the way platforms, employers, and brands secure advance consent through standard-form agreements. This section sketches the current landscape and highlights the blind spots that emerge once digital persona is treated as a licensable input for generative AI.

3.1 Judicial Recognition of Personality Rights

Indian courts have gradually recognised that an individual has a protectable interest in their persona, particularly where name, likeness, or voice is used without consent for commercial gain. Early cases framed this as an aspect of passing off and unfair competition, emphasising that a celebrity's identity carries distinct commercial value that third parties cannot exploit without permission. Later decisions explicitly connected this interest to the constitutional right to privacy and dignity under Article 21, noting that control over one's public image is part of personal autonomy. In recent litigation involving prominent actors and public figures, courts have granted wide-ranging injunctions against unauthorised use of names, images, or synthetic deepfakes for advertising or deceptive content, treating such conduct as an infringement of personality rights rather than merely a copyright or trademark issue.[14]

Despite these developments, the jurisprudence remains largely reactive and fact-specific. Relief is granted when a plaintiff can show clear unauthorised use of identifiable attributes in a specific context, such as a misleading advertisement or pornographic deepfake. The underlying doctrinal language still assumes a familiar pattern: an identifiable claimant, a recognisable persona, and a discrete instance of misuse that can be enjoined. What it does not yet squarely address is the situation in which the claimant ostensibly "consented" to broad

[14] Amitabh Bachchan v. Rajat Nagi, 2022 (6) HCC (Del) 641 (Del HC); Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Del HC).

exploitation of likeness or voice at an earlier stage through a standard-form contract, without meaningful negotiation or appreciation of AI-related downstream uses. Courts have not fully articulated when such consent should be considered invalid, unconscionable, or incompatible with core privacy and dignity interests.

3.2 Constitutional Privacy and Identity Autonomy

The Supreme Court's recognition of privacy as a fundamental right has provided a conceptual foundation for stronger control over personal identity. In its leading privacy decision, the Court described privacy as encompassing bodily integrity, informational self-determination, and the ability to control the projection of one's personality to the world. Commentators have read this as endorsing a notion of "identity autonomy," in which individuals have a constitutional stake in deciding how their attributes including name, image, or voice are collected, processed, and displayed.[15]

However, translating that high-level principle into the granular world of platform and employment contracts is not straightforward. The privacy judgment did not directly confront the problem of bundled, prospective consent in non-negotiable digital agreements, nor did it specify how far an individual may validly waive control over future manipulations of persona. In practice, privacy is enforced through statutes and sectoral regulations that focus on data processing rather than on the open-ended licensing of identity for commercial or AI-driven uses. As a result, there remains a gap between the Court's robust rhetoric on autonomy and the everyday reality in which users and workers routinely "agree" to terms that allow extensive reuse and transformation of facial or vocal data.

3.3 Data Protection: Strong on Processing, Weak on Persona

India's data-protection framework formally recognises harms such as identity theft, reputational damage, or loss of autonomy as cognisable injuries arising from misuse of personal data. Controllers are required to obtain consent, limit processing to specified purposes, and implement safeguards against unauthorised access or misuse. Provisions dealing with "harm" appear to include scenarios where personal data is used to impersonate or misrepresent an

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (SC); Anmol Arora, "Constitutional Protection of Personality Rights in the Era of Artificial Intelligence: A Comparative Study of India, EU and the US", International Journal of Multidisciplinary Research (IJFMR), Vol. 7, Issue 4 (2025).

individual, suggesting a potential route to challenge some AI-enabled abuses.[16]

Yet the central focus of data-protection law remains on processing data about individuals, not on creating new generative representations of persona. Once a person has consented—even in a broad click-wrap form to use of their data for "improvement of services" or "development of new features," it is not clear at what point training a model on their images or recordings becomes unlawful in itself. The law also does not clearly distinguish between processing that merely analyses data and processing that generates synthetic outputs capable of substituting for the person in future communications or endorsements. Moreover, data-protection obligations typically apply to entities formally designated as data fiduciaries or processors; they do not directly regulate the substance of private licensing clauses between employers, platforms, or creators, which may go far beyond what is strictly necessary for data processing.

3.4 The Consent Paradox

Taken together, these frameworks generate a consent paradox. On one hand, personality-rights and privacy jurisprudence suggest that individuals should have robust control over how identity is used, especially where commercial exploitation or dignitary harms are at stake. On the other hand, data-protection statutes and contract doctrine treat consent often expressed through standard-form terms as a central legitimising device. When a platform or employer points to a broad licence or assignment that purports to authorise AI training, cloning, or perpetual reuse of facial or vocal attributes, courts and regulators face a difficult question: is this a genuine exercise of autonomy, or an exploitative transaction that undermines the very personality and privacy interests the law seeks to protect?

Existing cases and commentary offer only partial guidance. They tend to focus on situations where there was no consent at all, or where the impugned use clearly exceeds the scope of an ordinary licence. They do not yet provide a systematic approach to evaluating when consent to identity exploitation, embedded within a complex contract, should be considered invalid, non-waivable, or subject to stricter scrutiny. Without such an approach, there is a risk that constitutional and statutory protections remain largely formal, while in practice the legal system continues to uphold agreements that convert digital persona into a one-time commodity. The next section argues that overcoming this paradox requires reconceptualising digital

[16] Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 2(1)(q) (India).

persona as a distinct subject of contracting, rather than as a subset of content or data, and calls for an identity-centric framework that can guide both private drafting and public regulation.

4. The Digital Persona in Contracts: Why "Data" and "Content" Are No Longer Enough

The emergence of generative AI has exposed a conceptual weakness at the heart of existing contracting practices: they assume that everything users and workers provide to platforms or employers can be safely treated as "content," "works," or "data." That assumption was manageable when reuse meant rebroadcasting a television commercial or hosting a video on multiple servers. It becomes untenable when the same contractual language authorises the extraction of biometric features and performance styles to construct digital personas capable of acting autonomously in the market.

4.1 From Content to Digital Persona

Traditional IP and media contracts were drafted around relatively static objects: a photograph, a film, a song, or a performance captured in a fixed recording. Once licensed or assigned, these objects could be reproduced or edited, but they did not transform into new embodiments of the person. Generative AI changes that calculus. When a platform trains models on a user's face or voice, it is no longer simply storing or sharing existing works. It is building a system that can generate outputs that convincingly imitate how that person appears or sounds, including in contexts never contemplated at the time of the original agreement.

Scholars have begun to argue that this transformation requires rethinking the line between data and persona. One influential account describes certain kinds of data, especially biometric and behavioural traces, as "data as likeness," because they allow third parties to reconstruct the appearance or style of an individual even without directly using traditional images or recordings.[17] In contractual terms, this means that what appears on paper as a licence to "use content" may in practice function as a licence to mine and reproduce the human behind that content. The digital persona that emerges is not merely a derivative work in the copyright sense. It is a simulacrum, able to enter into communications, endorsements, or performances that sit somewhere between a creative work and an extension of the self.

[17] Zahr Said Takhshid, "Data as Likeness", 112 Georgetown Law Journal (forthcoming 2024).

4.2 The Limits of Existing Legal Categories

Current legal categories struggle to capture this hybrid nature. Copyright and neighbouring rights focus on economic control over works and performances, not on the broader question of whether a person should be able to prevent others from fabricating new appearances or statements in their likeness. Data-protection law treats biometric identifiers and voice samples as sensitive personal data, but is geared towards regulating collection and processing, not the downstream creation of synthetic agents that mimic identity. Personality-rights jurisprudence recognises that name, image, or voice have commercial value and dignitary significance, yet has so far dealt mainly with discrete unauthorised uses rather than with AI-mediated replication authorised through broad licences.

When contracts conflate these domains, they create opportunities for overreach. A single clause that assigns "all rights" in a performance, or grants a platform the right to "create derivative works from user content," effectively collapses multiple interests into one: control over the original work, control over informational processing of personal data, and control over the generation of persona-based outputs. Without doctrinal guidance, drafters default to treating these interests as equally alienable. This may be defensible for a script or a logo, but it is far more troubling when the subject matter is a person's face or voice being repurposed into endlessly reproducible avatars.

4.3 Why Contractual Neutrality Is Illusory

It might be argued that if parties agree to broad language, the law should respect their freedom of contract. In practice, however, the appearance of neutrality disguises profound asymmetries. Platforms and large media entities typically possess detailed knowledge of AI capabilities and long-term monetisation strategies for persona-based technologies. Individual users, workers, or small creators generally do not. They encounter contracts as non-negotiable conditions of participation or employment, framed in generic IP and content terms that reveal little about the scope of possible AI uses. Even where there is some awareness of deepfakes or synthetic media, the practical implications of consenting to AI training and persona cloning are rarely explained, let alone priced into the bargain.

From a constitutional perspective, this raises doubts about whether such consent can be considered a genuine exercise of autonomy, particularly when the clauses purport to authorise

uses that strike at the core of personality and dignity. Indian privacy jurisprudence suggests that certain aspects of identity may warrant heightened protection and may not be fully waivable through standard-form contracts. At the same time, personality-rights analysis in the AI context underscores the risk that unexamined licences will allow long-term commercial exploitation of persona without ongoing involvement or fair compensation.[18] Without a clearer conceptual distinction between ordinary content and digital persona, private contracts will continue to erode personality protections in ways that are formally valid but substantively misaligned with the values underlying Article 21.

4.4 Towards an Identity-Centric Lens on Contracting

Recognising digital persona as a distinct object of legal concern does not require abandoning existing IP and data frameworks. It requires adding an identity-centric lens to contracting practices that deal with faces, voices, or avatars. Under such a lens, clauses that authorise AI training, cloning, or synthetic reuse of identifiable human attributes would be treated differently from routine content licences. They would need to be separately highlighted, temporally limited, and tied to specific purposes, with mechanisms for revocation or renegotiation as technology evolves.

This shift in perspective also has implications for judicial interpretation. When disputes arise over the scope of a licence or assignment, courts would be encouraged to ask not only what the words can literally bear, but also whether reading them to authorise extensive persona replication is consistent with constitutional commitments to dignity and autonomy. In marginal cases, ambiguities could be resolved in favour of preserving personality rights, rather than presuming that a general grant of "all rights" extends to technologically novel forms of identity exploitation.

The next section turns to comparative experiences in other jurisdictions, where lawmakers and scholars are beginning to grapple with similar questions. Their approaches to biometric data, publicity rights, or AI-generated likeness provide useful, though not directly transplantable, benchmarks for thinking about how Indian law might formalise an identity-centric approach to

[18] AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025; "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).

contracting in the era of generative AI.

5. Identity-Centric Contracting: A Proposed Framework for Indian Law

If digital persona is to be more than a residual concern folded into ordinary content and data clauses, Indian law needs a framework that treats contractual dealings with identity attributes as a special category. Identity-centric contracting provides such a framework. It does not prohibit licensing or commercial use of persona, but insists that these arrangements reflect the heightened dignitary and economic stakes involved whenever a contract authorises AI-enabled replication of human identity.[19]

5.1 Core Principles of Identity-Centric Contracting

An identity-centric approach rests on several interlocking principles that can guide both private drafting and public oversight:[20]

1. **Segregation and Salience of Persona Clauses** Permissions relating to digital persona should be clearly distinguished from general content or data licences. Any clause that authorises the use of facial images, voice recordings, or avatar-like depictions for AI training, cloning, or synthetic reuse should appear in a dedicated section, drafted in plain language, and flagged as requiring special attention. This mitigates the risk that consent to deeply intrusive uses of identity is buried within dense boilerplate.

2. **Purpose-Bound and Time-Bound Licensing** Licences over digital persona should be tied to specific, articulated purposes such as a campaign or production, and limited in duration. Open-ended phrases like "for any and all purposes" or "in perpetuity" are ill-suited where persona-based AI can generate new uses long after the original relationship has ended. A default presumption of time-limited licences, subject to renewal, would better align with expectations of ongoing control over one's identity.

3. **Separate, Specific Consent for AI Training and Cloning** Any use of identifiable persona in training generative models or in creating autonomous synthetic

[19] AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025.

[20] Anmol Arora, "Constitutional Protection of Personality Rights in the Era of Artificial Intelligence: A Comparative Study of India, EU and the US", International Journal of Multidisciplinary Research (IJFMR), Vol. 7, Issue 4 (2025).

performances should require separate consent, distinct from the consent to publish or reuse the original content. This consent should describe, at minimum, the nature of the models to be trained, the types of outputs envisaged (for example synthetic voice overs or virtual avatars), and whether those outputs may be used independently of the person's future involvement. Without such specificity, "improvement of services" clauses risk collapsing into a general authorisation for personality replication.[21]

4. **Residual Control and Revocability** Contracts should recognise that some aspects of digital persona cannot be fully alienated without undermining core interests in dignity and autonomy. Where feasible, individuals should retain a right to withdraw consent for future synthetic uses, subject to reasonable notice and consideration of reliance interests. Even where past outputs cannot be recalled, revocation can prevent further training or deployment of models built on the person's likeness or voice.[22]

5. **Fair and Ongoing Compensation** When a contract permits the creation of autonomous AI avatars or synthetic voice performances that continue to generate value, it is rarely sufficient to treat the underlying persona as a one-time input. Identity-centric contracting supports remuneration models that link payment to the duration or intensity of synthetic use, such as royalties tied to campaigns, impressions, or revenue. This helps ensure that commercial benefits from AI-mediated exploitation of persona are not entirely captured by platforms or producers.[23]

6. **Non-Waivable Minimum Standards** Certain safeguards should be treated as non-waivable, especially in standard-form contracts. These could include prohibitions on using a person's digital persona in contexts that are degrading or defamatory, or in ways incompatible with fundamental rights, even if a broad licence was granted. Indian constitutional jurisprudence already recognises that there are limits to what individuals can consent to where core dignity is at stake; identity-centric contracting would translate that insight into concrete contractual constraints.[24]

[21] "AI Training Models and Website Terms of Use", Chip Law Group, 18 September 2023.
[22] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (SC).
[23] "Expert Take: Publicity, Privacy and Performance Rights", Economic Times – Legal, 9 November 2025.
[24] Amitabh Bachchan v. Rajat Nagi, 2022 (6) HCC (Del) 641 (Del HC); R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (SC).

5.2 Operationalising the Framework in Practice

Implementing these principles does not require every contract to become a bespoke negotiation. Instead, they can be reflected through standard drafting practices and institutional guidance:

- **Model Persona Clauses** Industry bodies, bar associations, or regulators can promote model clauses that embody identity-centric standards, offering a baseline against which more restrictive language can be scrutinised. Guidance on performance and publicity rights in the AI context already points toward the need for clearer drafting around digital replicas and synthetic uses.[25]

- **Layered Consent Design** Platforms and employers can adopt layered consent flows where persona-related permissions are presented separately from general terms, with simplified summaries and examples of AI uses. This would mirror best practices in data-protection consent design for high-risk processing of biometric data, adapted to the contractual sphere.[26]

- **Judicial Interpretation** Courts, when faced with disputes over the scope of licences or assignments, can interpret ambiguous provisions narrowly where they purport to authorise novel forms of persona replication, and can treat the absence of clear, specific consent as weighing against such expansive readings. Indian decisions on personality rights already show a willingness to protect identity interests robustly where contractual language is unclear or exploitative.[27]

Taken together, these measures would begin to correct the current imbalance, in which personality rights and privacy are asserted at a high level while everyday contracts quietly erode control over digital persona. The next section turns from principles to regulatory levers, examining how intermediary rules, data-protection implementation, advertising standards, and labour regulation in India could be adapted to embed identity-centric contracting into the positive law of the platform and creator economy.

---

[25] "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 7, 9.
[27] Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Del HC); D.M. Entertainment Pvt. Ltd. v. Baby Gift House, MANU/DE/2043/2010 (Del HC).

6. Regulatory Levers: Embedding Identity-Centric Contracting into Indian Law

Translating identity-centric contracting from principle to practice requires more than voluntary private law reform. In India's highly intermediated digital ecosystem, regulators and self-regulatory bodies already shape the terms on which platforms, employers, and advertisers operate. These existing levers can be adapted to ensure that contractual dealings with digital persona meet minimum standards of transparency and fairness, with consent treated as a distinct requirement.

6.1 Intermediary Rules and Platform Obligations

Information technology regulation in India conditions safe-harbour protections for intermediaries on compliance with due-diligence obligations, including grievance redressal, notice-and-takedown mechanisms, and disclosure duties. Recent amendments have expanded these responsibilities in response to deepfakes and harmful content, signalling a willingness to impose more substantive obligations on platforms that host and algorithmically amplify user-generated media.[28]

Identity-centric contracting could be integrated into this framework in two ways. First, intermediary guidelines could require "significant" social media and AI platforms to adopt separate, explicit disclosures whenever their terms of service authorise the use of user images or audio for AI training or persona-based features. Such disclosures could be treated as part of due diligence, with regulators empowered to question vague formulations like "improve our services" where they mask far-reaching personality-related uses. Second, safe-harbour status could be tied to the existence of robust, user-friendly mechanisms for revoking consent to future persona-based AI uses, even where the original terms purported to grant broad licences. This would not retroactively outlaw past processing, but would prevent ongoing deployment of AI models that continue to exploit a person's likeness or voice against their wishes.

6.2 Data Protection Implementation and High-Risk Persona Processing

India's data-protection regime treats identity theft and reputational harm as cognisable injuries arising from misuse of personal data, and recognises that certain categories, such as biometric

[28] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended; AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025.

identifiers, warrant heightened protection.[29] Implementation rules and sectoral codes of practice can build on this recognition by explicitly classifying AI training and generation involving identifiable faces or voices as a form of high-risk processing.

For contracts, this would mean that any clause purporting to authorise such processing must meet stricter standards of granular, informed consent, akin to those expected for sensitive data processing under comparative data-protection regimes. Regulators could issue guidance clarifying that bundled consent in standard-form agreements is inadequate where it covers training or deployment of models that can generate synthetic speech or images closely resembling a real person. Controllers relying on consent would need to demonstrate that individuals were given a genuine choice, with clear explanations of the nature and implications of persona-based AI uses. This would indirectly push contracts toward the separate, specific consent model advocated by identity-centric contracting.

6.3 Advertising and Self-Regulation: Synthetic Endorsements

The Indian advertising ecosystem is already subject to self-regulatory codes that prohibit misleading endorsements and require truthful representation of celebrity associations with products. Recent commentary has extended these concerns to AI-generated endorsements and deepfake commercials, emphasising the potential for consumer deception when synthetic media is used to simulate a human recommender.[30]

Self-regulatory bodies could update their codes to address digital persona explicitly. For instance, guidelines could require advertisers and agencies to obtain documented, persona-specific consent before using AI to create or modify endorsements that depict a recognisable person, including influencers or actors. They could also require clear on-screen disclosure when AI is used to simulate or alter a person's appearance or voice in an advertisement. Such standards would, in practice, force brand-side contracts to incorporate identity-centric clauses, since non-compliant campaigns could trigger reputational sanctions or removal.

6.4 Labour and Sectoral Regulation: Protecting Performers and Platform Workers

Labour and sector-specific regulation provide a further avenue for embedding identity-centric

[29] Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 2(1)(q) (India).
[30] "Expert Take: Publicity, Privacy and Performance Rights", Economic Times – Legal, 9 November 2025.

contracting. Performers' unions and guilds in other jurisdictions have already negotiated contractual limits on AI cloning of actors and voice artists, including requirements for separate consent and additional compensation.[31] While India's creative and platform work sectors are more fragmented, there is scope for statutory or quasi-statutory norms that set minimum standards for contracts involving digital persona.

In the film, television, and advertising industries, sectoral rules or model contracts endorsed by regulators or industry bodies could stipulate that assignments of rights in performances do not, by default, include AI-based cloning or generation of new performances, unless separately and specifically agreed with appropriate remuneration. For platform workers and online creators, labour authorities could encourage or require platforms to offer default terms that exclude perpetual persona licences as a condition of access, particularly where workers lack realistic alternatives. Such measures would not prevent more sophisticated parties from negotiating broader uses, but would ensure that the baseline for vulnerable workers does not involve wholesale alienation of digital persona.

6.5 Coordinated Governance and Enforcement

Finally, embedding identity-centric contracting will require coordination among multiple institutions, including technology regulators, data-protection authorities, advertising self-regulators, and labour bodies, to avoid gaps and overlaps. Comparative experience with AI regulation suggests that fragmented oversight can leave individuals without clear avenues for redress when synthetic persona exploitation spans several domains at once.[32] Indian regulators can pre-empt this by establishing joint working groups or memoranda of understanding that recognise digital persona as a cross-cutting issue and allocate responsibilities for monitoring contractual practices, issuing guidance, and handling complaints.

Together, these regulatory levers would begin to realign the legal environment in which digital persona licensing occurs. Instead of leaving the shape of personality rights in the AI era entirely to private drafting, Indian law would signal that certain structural features—clear consent,

[31] "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).

[32] Anmol Arora, "Constitutional Protection of Personality Rights in the Era of Artificial Intelligence: A Comparative Study of India, EU and the US", International Journal of Multidisciplinary Research (IJFMR), Vol. 7, Issue 4 (2025).

limited duration, revocability, and fair reward—are not optional extras but part of the basic architecture of lawful contracting over human identity. The concluding section draws these strands together and reflects on the broader implications of this shift for the future of personality rights in India's platform economy.

7. Risks, Objections, and Safeguards

Identity-centric contracting is not cost-free. Any proposal to re-engineer the contractual treatment of digital persona will encounter objections from platforms, brands, and some creators who benefit from frictionless reuse of content. This section anticipates concerns and sketches safeguards that can keep the framework proportionate and workable.

7.1 Innovation and Compliance Burdens

A common objection is that additional consent flows, segregation of clauses, and mechanisms for revocation will raise transaction costs and slow innovation, especially for smaller firms that rely on streamlined terms of use. Platforms may argue that granular persona clauses are impractical at scale and that rigid limits on AI training would impair their ability to improve recommendation systems or offer new features.

Identity-centric contracting can accommodate these concerns through risk-based calibration. The most stringent requirements separate consent, time-bounded licences, and revocation rights can be focused on clearly persona-intensive uses, such as training generative models capable of producing realistic synthetic faces or voices, or deploying avatars in commercial communications. Lower-risk uses, like non-identifiable analytics or basic content optimisation, can remain under simpler consent structures. Moreover, many of the proposed changes (for example, splitting persona clauses into a separate section or adding a dashboard toggle for future AI training) involve modest design and drafting adjustments rather than ongoing bureaucratic oversight, in line with broader proportionate regulation approaches adopted in AI and data governance discussions.[33]

[33] Anmol Arora, "Constitutional Protection of Personality Rights in the Era of Artificial Intelligence: A Comparative Study of India, EU and the US", International Journal of Multidisciplinary Research (IJFMR), Vol. 7, Issue 4 (2025).

7.2 Consent Fatigue and User Overload

Another concern is that requiring separate, explicit consent for persona-based AI uses will exacerbate "consent fatigue," leading users to click through additional prompts without real understanding. If every platform and employer introduces multiple consent layers, the protective value of those layers may erode.

Here, the design of consent mechanisms becomes crucial. Rather than multiplying fine-print checkboxes, identity-centric contracting encourages fewer but more meaningful consent events for high-impact uses. Well-designed interfaces can present concrete examples of what persona-based AI entails, such as "creating a digital avatar that can speak in your voice in future campaigns," using simple language and visual aids. Regulatory guidance on high-risk biometric and AI processing already emphasises the importance of layered, intelligible consent for complex technologies; a similar philosophy can be applied at the contract level so that the framework improves the quality, not just the quantity, of consent.[34]

7.3 Regulatory Fragmentation and Overlap

Because digital persona touches multiple domains, including platform regulation, data-protection, advertising law, and labour, there is a risk that overlapping rules will create uncertainty and inconsistent obligations. Businesses may fear a patchwork of standards, each enforced by different authorities, leading to regulatory arbitrage or paralysis.

This risk can be mitigated through coordinated standard-setting. Cross-sectoral working groups or consultative processes can produce joint guidelines that articulate a common set of expectations for persona-related contracting: clear segregation of clauses, specific consent for AI training and synthetic use, baseline dignity safeguards, and mechanisms for revocation and redress. Different regulators can then implement these principles within their own mandates, but against a shared conceptual backdrop. Comparative accounts of AI governance stress that such coordination is essential to avoid regulatory voids around synthetic identity, where no single body feels responsible for contractual practices that enable persona exploitation.[35]

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 7, 9.
[35] "AI Innovations and their Impact on Personality Rights", 31 Journal of Intellectual Property Rights (CSIR-NIScPR, 2026).

7.4 Over-Protection and Chilling Effects

A further objection is that strong identity-centric safeguards might over-protect persona, chilling legitimate uses such as satire or artistic transformation. If every depiction of a recognisable individual requires detailed contractual consent, important expressive and cultural activities could be stifled.

The proposed framework need not extend that far. It is primarily directed at contractual licensing in commercial and platform settings, especially where AI is used to create substitutable synthetic performances. It does not suggest that all incidental or non-commercial depictions of individuals should be contractually regulated. Existing defences and exceptions for news reporting, commentary, and parody can continue to operate, and statutory or judge-made limits on personality-rights claims can be preserved. The focus of identity-centric contracting is on circumstances where a person's face or voice is transformed into an ongoing economic asset for others, not on ordinary public discourse or artistic engagement, which comparative scholarship on personality rights and free expression identifies as an area calling for careful balancing rather than absolute control.[36]

7.5 Safeguards Against Formalism

Finally, there is a danger that identity-centric contracting could degenerate into a formalistic box-ticking exercise, with platforms and employers complying in letter but not in spirit. If persona clauses become just another set of standard lines inserted without real negotiation or explanation, the framework may do little to change underlying power dynamics.

Addressing this requires interpretive and enforcement safeguards. Courts and regulators can treat the presence of formally correct clauses as a starting point, not an end point, scrutinising whether consent was genuinely informed and whether the overall contractual balance is consistent with constitutional commitments to dignity and autonomy. In egregious cases, for example where a vulnerable worker has "agreed" to extremely broad persona exploitation under economic duress, doctrines of unconscionability, public policy, or statutory consumer protection can be invoked to refuse enforcement. Indian decisions on personality rights and privacy already demonstrate judicial willingness to look beyond formal consent where core

[36] AI, Identity and Law: Personality Rights in India and US – Comparative Study in the Digital Age, Legal Era, 21 December 2025.

aspects of identity and dignity are threatened.[37] Over time, such interventions can signal that identity-centric contracting is not merely a drafting fashion, but a substantive expectation about how human identity may be treated in the platform economy.

Taken together, these safeguards demonstrate that the risks associated with identity-centric contracting are real but manageable. With careful calibration, India can strengthen contractual protection for digital persona without paralysing innovation or drowning users and workers in meaningless consent prompts. The concluding section turns to the broader stakes of this project and the role it can play in shaping the future relationship between human identity and AI in the Indian legal order.

8. Conclusion: Keeping Humans Ahead of Their Digital Doubles

The rise of generative AI has exposed a structural weakness in the way Indian law treats human identity. Courts and statutes recognise personality and privacy as important interests, yet the everyday contracts that govern life on platforms or in creative industries still treat identity attributes as ordinary "content" or "data." Identity is thus quietly transformed into a licensable input for AI systems that can generate synthetic doubles, including avatars or cloned voices, capable of acting in the market without the person's ongoing participation, consent, or remuneration.

This article has argued that such developments cannot be managed solely through ex post litigation over deepfakes or unauthorised endorsements. Doctrines of personality rights, constitutional privacy, and data protection, though vital, were not designed to evaluate bundled, forward-looking consent to AI-driven persona replication embedded in standard-form agreements. Without a complementary contractual framework, there is a real risk that formal consent will routinely override substantive autonomy, leaving individuals bound by licences they neither fully understood nor had the power to negotiate.

Identity-centric contracting offers a way to realign private agreements with the values that Indian law already professes. By insisting on segregation and salience of persona clauses, specific and revocable consent for AI training and synthetic use, time-bound and purpose-bound licences, fair ongoing compensation, and non-waivable dignity safeguards, it

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (SC); Amitabh Bachchan v. Rajat Nagi, 2022 (6) HCC (Del) 641 (Del HC).

recognises that digital persona sits at the intersection of economic livelihood and constitutional dignity. When embedded through platform obligations, data-protection implementation, advertising standards, or labour norms, these principles can shift the default from personality capture to personality stewardship, without freezing innovation.

What is ultimately at stake is the basic relationship between human beings and their technologically mediated representations. If contracts and regulation remain anchored in an information-age conception of "content," Indian creators, workers, and users may find themselves competing in markets or feeds against synthetic versions of themselves that others control. An identity-centric approach does not seek to halt AI's advance, but to ensure that as digital doubles become more capable, the law keeps its normative focus on the originals: the human persons whose faces or voices remain the source of all value in the identity-replication economy.