

The Price of Privacy: A Hybrid Model for Data Protection in Indian Insolvency Law

*Madhumitha Shankar**

ABSTRACT

The isolated operations of the Insolvency and Bankruptcy Code, 2016 (I&B Code) and the Digital Personal Data Protection Act, 2023 (DPDP Act) precipitate a legal vacuum at the intersections of insolvency and privacy. This paper identifies and explores the competing objectives of the I&B Code and the DPDP Act, particularly with respect to the sale of consumers' personal data as a part of the resolution plan or liquidation proposal of the corporate debtor. It adopts comparative analysis as its primary methodology in analysing the treatment of personal data during insolvency. It extrapolates from the jurisdictions of the European Union (EU) and the United States of America (US). While the EU model has stronger data protection mechanisms grounded in a constitutional right to privacy, the US model benefits from procedural flexibility that allows for the derivation of greater economic benefits. Adopting economic pragmatism, the paper argues for a hybrid three-tiered model optimised for the

* Madhumitha Shankar is a fourth-year BA, LLB (Hons) student at National Law University, Delhi. The author may be contacted at madhu.mithas22@nludelhi.ac.in.

Indian context. It rests on the differential and nuanced treatment of distinct categories of data on the basis of their nature and sensitivity. The paper concludes with a call for legislation that incorporates such a model into Indian law, thereby harmonising the insolvency and privacy frameworks while passing the test of constitutionality set out in the Puttaswamy judgement. It contributes to the discourse on insolvency laws by addressing a critical legal blind spot that becomes increasingly important due to the age of digitalisation. In doing so, it presents both value-maximisation of the debtor’s assets and protection of consumers’ data as important commitments that need to be balanced through unambiguous and pragmatic legislation.

TABLE OF CONTENTS

| | | |
|------|--|-----|
| I. | Introduction..... | 120 |
| II. | Personal Data as an Asset in Insolvency..... | 122 |
| III. | Comparative Perspectives from Foreign Jurisdictions..... | 126 |
| A. | European Union | 126 |
| B. | United States of America..... | 130 |
| IV. | Way Forward for India..... | 134 |
| V. | Conclusion | 140 |

I. INTRODUCTION

The Insolvency and Bankruptcy Code, 2016 (**I&B Code**), India's comprehensive legislation on the reorganisation and resolution of distressed entities, was enacted with the stated objectives of maximisation of value of assets of debtors, promotion of entrepreneurship and availability of credit, and balancing of the interests of all the stakeholders.¹ However, the establishment of a creditor-oriented bankruptcy regime² calls into question the I&B Code's capacity to adequately consider the interests of *all* the stakeholders, especially in cases involving personal data as assets. Where a company that collects and stores consumer data is involved in a corporate insolvency resolution process (**CIRP**), the data in the possession of the debtor comes to be viewed as an 'asset' whose value must be maximised to increase creditor benefits. This precipitates a confrontation between the I&B Code and the **DPDP Act**, which is the primary legislation on the processing of personal data in India. However, the contours of the interplay between the I&B Code and the DPDP Act are unspecified and underexamined due to the silence of both legislations on the treatment of personal data during insolvency. Thus, in India, there is no framework for how the interests of the debtor and creditors on one hand, and the interests of the Data Principals on the other, are to be balanced.

This creates a critical blind spot in insolvency jurisprudence, and a concrete explication regarding privacy concerns in insolvency

¹ Insolvency and Bankruptcy Code 2016 (**IBC 2016**).

² Amol Baxi, 'Interim Finance in Creditor-Oriented Bankruptcy Codes: A Study in the Context of Insolvency & Bankruptcy Code, India' (2023) 48 *Vikalpa: The Journal for Decision Makers* 189-205.

proceedings becomes increasingly urgent given the rising significance of data in today's digital global landscape. With the rapid digitisation of business processes in recent decades, data is well-established as 'informational goods', and is treated as a quantifiable asset.³ Further, data is monetised to generate profit, either by selling it directly or utilising it to create value indirectly.⁴ Since intangible assets tend to appreciate over time, data is often the most valuable asset of the debtor during insolvency.⁵ In this context, the ambiguity in the treatment of personal data as an asset during the CIRP can lead to catastrophic consequences for Data Principals. This paper addresses this legal vacuum, grounding its approach on the argument that both privacy and value-maximization are co-equal commitments that require pragmatic harmonization. First, it lays down the conceptual framework for personal data as an asset during insolvency proceedings, critically analysing the lacunae in the legislation as well as omissions in real-world insolvency cases. Second, it offers comparative perspectives from the jurisdictions of the EU and the US. This section analyses the de jure status of data in these jurisdictions, as well as their method of dealing with the opposing tensions between insolvency and privacy. Finally, the paper proposes a three-tiered model, drawing from both the EU and US approaches, and optimally reconfigured for the Indian context. It demonstrates that such legislation passes the test of constitutionality prescribed in the

³ Jian Pei, 'A Survey on Data Pricing: From Economics to Data Science' (2022) 34 IEEE Transactions on Knowledge and Data Engineering 4586.

⁴ Abou Zakaria Faroukhi and others, 'Big data monetization throughout Big Data Value Chain: a comprehensive review' (2020) 7 Journal of Big Data 3 <<https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0281-5>> accessed 24 October 2025.

⁵ Cameron Love, 'Data in Distress: Effectuating State Data Privacy Laws During Bankruptcy' (2024) 73 Emory L J 1061.

Puttaswamy case,⁶ and concludes with a call for legislative action that incorporates and legitimises this model.

II. PERSONAL DATA AS AN ASSET IN INSOLVENCY

The question of whether personal data is to be treated as an asset of the corporate debtor in the CIRP must be analysed in terms of two basic inquiries: what is ‘personal data’ under the DPDP Act? What is an ‘asset’ under the I&B Code?

Personal data is defined under the DPDP Act as “any data about an individual who is identifiable by or in relation to such data”.⁷ As per the statutory scheme, data is not ‘owned’ by the company; instead, the company is a Data Fiduciary⁸ who holds the data in a regulated, fiduciary capacity on behalf of the data principal, that is, the individual to whom the personal data relates.⁹ The Act specifically avoids the language of ownership, and instead frames the de jure status of data in terms of rights, duties, and permissions. Further, it does not confer property rights over personal data, or provide for its alienation, sale or transfer of ownership. Data is presented as a bundle of limited rights held by the data principal, such as the right to access information about personal data,¹⁰ the right to correction and erasure,¹¹ and the right of grievance redressal.¹² Data fiduciaries, on the other hand, do not acquire rights *in rem* over the personal data, but only entitlements to process data on the

⁶ *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

⁷ Digital Personal Data Protection Act 2023 s 2(t) (**DPDPA 2023**).

⁸ DPDPA 2023, s 2(i).

⁹ DPDPA 2023, s 2(j).

¹⁰ DPDPA 2023, s 11.

¹¹ DPDPA 2023, s 12.

¹² DPDPA 2023, s 13.

grounds of the Data Principal's consent, or for certain legitimate uses.¹³ However, practice indicates that there is a functional commodification without formal ownership, as data fiduciaries are capable of monetising and monopolising personal data.¹⁴

The legal status of data under the DPDP Act differs from the legal status of data under the I&B Code. An inclusive understanding of 'asset' can be inferred from Section 18 of the I&B Code, which directs the interim resolution professional to 'take control and custody of any asset over which the corporate debtor has ownership rights', including 'intangible assets, including intellectual property'.¹⁵ On a *prima facie* view, 'intangible assets' can be construed to include customer databases, user behaviour analytics, and other forms of monetizable personal data in the corporate debtor's possession, especially when they form the core of the debtor's business process. However, this is further complicated by the Explanation appended to Section 18, which provides that 'assets' shall not cover 'assets owned by a third party in possession of the corporate debtor held under trust or under contractual arrangements including bailment'.¹⁶

This brings forth an ambiguity in the law: if personal data under the DPDP Act's framework is not 'owned' by the data fiduciary/corporate debtor in the traditional sense, but only held in possession and processed subject to regulation, then it is not an asset that the resolution

¹³ DPDPA 2023, s 4.

¹⁴ Ajay Kumar Bisht and Neeruganti Shanmuka Sreenivasulu, 'Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023' in Jaydip Sen (ed), *Data Privacy – Techniques, Applications, and Standards* (IntechOpen 2025).

¹⁵ IBC 2016, s 18(f).

¹⁶ IBC 2016, s 18, Explanation.

professional is empowered to control or alienate under the I&B Code. A clear answer to this ambiguity is crucial to setting the legal boundaries of asset monetization in the CIRP.

Clarification of the legal status of personal data as an asset during insolvency becomes even more pertinent and compelling due to this conflict already emerging as a legal blind spot in recent CIRP proceedings. For example, in the *Jet Airways insolvency* case in 2019, the corporate debtor's reported assets included fourteen (14) aircrafts and a 49.9% stake in the JetPrivilege programme,¹⁷ which was constituted with the primary purpose of developing a 'data-driven customer engagement platform'.¹⁸ Evidently, passenger data from the loyalty programme was 'heavily discussed in negotiations' as a saleable asset.¹⁹ However, the personal data itself was not itemised as a separate asset. Instead, assenting financial creditors were offered a 7.5% stake in JetPrivilege in the approved resolution plan.²⁰ The silence on data is concerning because it demonstrates the unscrutinised and undefined status of personal data even in data-rich businesses. This omission

¹⁷ Press Trust of India, 'Jet Airways lenders plan to call bids for asset sale by Saturday' *India Today* (Mumbai, 17 July 2019) <<https://www.indiatoday.in/business/story/jet-airways-lenders-call-bids-sell-assets-1570241-2019-07-17>> accessed 24 October 2025.

¹⁸ Ajita Shashidhar, 'How JetPrivilege transitioned from loyalty programme to consumer tech business InterMiles' *Business Today* (14 February 2020) <<https://www.businesstoday.in/industry/aviation/story/how-jetprivilege-transitioning-loyalty-programme-consumer-tech-business-250148-2020-02-14>> accessed 24 October 2025.

¹⁹ Agrud Partners, 'Airline Insolvency in India: Legal Gaps in Lessors' Rights and Passenger Data Protection' (*Legal 500*, 10 June 2025) <<https://www.legal500.com/developments/thought-leadership/airline-insolvency-in-india-legal-gaps-in-lessors-rights-and-passenger-data-protection/>> accessed 24 October 2025.

²⁰ *SBI v Jet Airways (India) Ltd* [2021] SCC OnLine NCLT 11967.

signals that insolvency institutions do not regard personal data as a discrete, legally protected asset and neglect to ensure explicit data protection, even though it is governed by fiduciary obligations under the DPDP Act.

Another instance is the CIRP of Karvy Data Management Services (**KDMS**), which was initiated in 2023.²¹ KDMS was essentially a data-processing firm dealing in sensitive data such as Aadhaar details,²² which means that its principal asset was customer data held under fiduciary obligations. The resolution plan was approved by the Hyderabad bench of the National Company Law Tribunal (**NCLT**) for an amount of Rs. 158.56 crores.²³ However, there was no specificity in the plan that accounted for the distinct nature of personal data. Again, the omission points to the overlooking of personal data in insolvency proceedings, and a certain level of laxity in its treatment not befitting the regulations imposed by the DPDP Act.

Thus, the lack of explicit procedural and substantive safeguards for the protection of personal data during insolvency processes within the DPDP Act, and the absence of clear directives on the monetisation of personal data within the I&B Code, creates scope for the transgression of the privacy rights of data principals during the resolution or liquidation of a data fiduciary/corporate debtor. Despite the prominent role of consumer

²¹ Pallavi Mishra, 'KYC And Aadhaar Related Service Provider 'Karvy Data Management Services Ltd.' Admitted Into Insolvency: NCLT Hyderabad' (*LiveLaw*, 21 September 2023) <<https://www.livelaw.in/ibc-cases/kyc-and-aadhaar-related-service-provider-karvy-data-management-services-ltd-admitted-into-insolvency-nclt-hyderabad-238337>> accessed 24 October 2025.

²² Karvy Data Management Services, (*Karvy KRA*) <<https://www.karvykra.com/>> accessed 14 June 2025.

²³ *Allied Hi-Tech Industries (P) Ltd v Karvy Data Management Services Ltd* [2024] SCC OnLine NCLT 3827.

data in profit-generation and value-maximisation, the I&B Code is entirely silent on the status of personal data as an ‘asset’ for the purposes of CIRP. Further, it ignores the fiduciary character of personal data. This engenders the violation of the right to privacy under Article 21 of the Indian Constitution. Further clarification regarding this legal lacuna is absolutely critical not only to harmonise the privacy and insolvency regimes, but also to protect the constitutional rights of persons in India.

III. COMPARATIVE PERSPECTIVES FROM FOREIGN JURISDICTIONS

An overview of the treatment of personal data during insolvency in foreign jurisdictions helps conceptualise a solution suitable for the Indian legal framework. This paper extrapolates from jurisprudence in the EU and the US, engaging with them on the question: how do these jurisdictions conceptualise personal data in relation to its commercialisation? And how do they seek to regulate the transfer of personal data during insolvency proceedings? It argues that while the EU model is normatively superior in terms of protection of privacy rights, the US model possesses a level of procedural flexibility that is required for efficient resolution. In the final analysis, a hybridisation borrowing desirable principles from each model is best suited in the Indian context, which commands constitutional protection of privacy rights as well as statutory guarantee of value maximisation for insolvents.

A. European Union

The EU attaches a strong legal and cultural significance to privacy and data protection, as evidenced by the institutionalisation of these norms in the European Charter of Fundamental Rights. Article 8 of the Charter

explicitly confers the right to the protection of personal data.²⁴ It also sets forth the purpose limitation principle, which requires the use of personal data to be limited to the specific purposes for which it was collected.²⁵ It also permits processing of data based on consent, or for legitimate reasons laid down by law, similar to the Indian DPDP Act.²⁶ Thus, the data protection framework is heavily entangled in the constitutional right to privacy in the EU. The EU views personal data as an extension of the data subject's legal personality, thus excluding conventional notions of ownership over personal data.²⁷

The significance of such an understanding of personal data for the context of insolvency is that, in the trade-off between privacy rights and the commercial value of data, citizens' rights generally trump the economic interests of the insolvent company. This approach is codified in the General Data Protection Regulation (**GDPR**), the supranational European law on the governance of data. It allows processing of personal data for certain reasons mentioned in Article 6. However, the entitlement to process data is merely a 'usage right over the personal data as a license', and does not entail transfer of 'ownership' of personal data from the data subject to the company.²⁸

²⁴ Charter of Fundamental Rights of the European Union [2012] OJ C326/391 art 8(1) (**CFR**).

²⁵ **CFR**, art 8(2); Valery Gantchev, 'Data Protection in the Age of Welfare Conditionality: Respect for Basic Rights or a Race to the Bottom?' (2019) 21 *Eur J Soc Sec* 3.

²⁶ **CFR**, art 8(2).

²⁷ Bart Van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'' (2015) 31 *Utrecht J Int'l & Eur L* 25.

²⁸ Ronny Hauck, 'Personal Data in Insolvency Proceedings: The Interface between the New General Data Protection Regulation and (German) Insolvency Law' (2019) 16 *European Company and Financial Law Review* 724.

In the context of insolvency, data processing is permissible if the data subject has given consent, or in the absence of consent, for the other sub-clauses in Article 6. The conditions for consent are specified in Recital 32 of the GDPR. It is framed in terms such as ‘unambiguous indication’ and ‘clear affirmative action’,²⁹ implying that consent required some positive and overt act. In the German *Unister insolvency* case, the Consumer Authority sued the buyer and the insolvency trustee on the grounds that explicit consent is essential for the processing of data, and silence does not amount to consent.³⁰ In the Dutch *TravelBird bankruptcy* case, that transfer would be permissible if consumers were informed in advance and given an opportunity to object. However, this would not be a transfer on the basis of consent, but on the basis of legitimate interest, signifying that consent as a ground requires something more than silence.

Moreover, the consent is only on the basis of the principle of purposive limitation. This ensures that preliminary consent at the time of obtaining the data is not sufficient. Further, the onus is on the data controller/insolvent company to demonstrate that the consent was actually given by the data subject.³¹ The data controller is also responsible for making a reasonable effort to verify that such consent is lawful.³² Thus, consent under the GDPR is heavily constrained, creating difficulties for the insolvent company in the sale or transfer of usage rights over consumer data.

²⁹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 recital 32 (GDPR).

³⁰ Hauck (n 28).

³¹ GDPR, art 7(1).

³² GDPR, art 8(2).

Other than consent, insolvent firms have sought to justify the transfer of usage rights over personal data on three other grounds. First, that ‘processing is necessary for a legal obligation on the data controller’,³³ however, it has been clarified that the legal obligation must be connected with data protection; hence, this clause cannot be used as a justification for transfer without the data subject’s consent.³⁴ Second, that ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’,³⁵ but this, too, is untenable as the insolvency administrator does not work in the public interest, and is not an official authority.³⁶ Third, that ‘processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party’.³⁷ This is tempered by the restrictions imposed in the same clause, and therefore entails a case-by-case balancing act between the interests of the debtor and creditors, and of the data subject.³⁸

Overall, in the EU context, the privacy regime acquires primacy over the insolvency regime because personal data is envisaged as an extension of the data subject’s personality, and not as an asset capable of being ‘owned’. Further, data protection is enforced through a state-market regulatory framework that envisages the ex ante formulation of rules that are grounded in the constitutional right to privacy, autonomy, and

³³ GDPR, art 6(1)(c).

³⁴ Hauck (n 28).

³⁵ GDPR, art 6(1)(e).

³⁶ Hauck (n 28).

³⁷ GDPR, art 6(1)(f).

³⁸ Hauck (n 28).

dignity.³⁹ However, this destroys the value of personal data as a means to save insolvent companies, and completely disregards the role and importance of its larger financial benefits in sustaining the economy. In the era of digitalisation, such legal rigidities may prove fatal to the goals of encouraging entrepreneurship and ensuring credit availability.

B. United States of America

The US approach differs considerably from the EU one. In the first place, the right to privacy is not explicitly guaranteed by the Constitution. Instead, it has been inferred from a patchwork of Amendments and judicial decisions which have held that the penumbras of the First, ninth and fourteenth amendments create a ‘zone of privacy’ protected Constitutionally.⁴⁰ However, the lack of a solid foundation renders it vulnerable to judicial discretion, and the strength of the right to privacy remains contingent on jurisprudential philosophy. Consequently, the data privacy regime in the US is weaker than the EUs’.

Partly, this is attributable to the US legal system’s socio-technical imagination of data as a monetizable asset.⁴¹ The problem of data privacy is framed in terms of the rights of persons versus the larger socioeconomic benefits derived from the commercialisation of data.⁴² Since the privacy rights framework has not been crystallised in the US, the latter takes a slight, but noticeable, precedence over the former. This

³⁹ Rob Guay and Kean Birch, ‘A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008-2016)’ (2022) 9 *Big Data & Society*.

⁴⁰ *Griswold v Connecticut* 381 US 479 [1965].

⁴¹ Guay and Birch (n 40).

⁴² *ibid.*

is particularly true for insolvency contexts, which are governed by the federal-level Bankruptcy Code.

Discourse at the intersections of privacy and insolvency was first introduced to the US legal climate in the *Toysmart case*. Toysmart.com, an e-commerce site for the sale of educational toys, had promised in its privacy policy that consumer data would ‘never be shared with third parties’.⁴³ However, when the company became insolvent in 2000, it attempted to sell its customer database during liquidation under Chapter 11 of the Bankruptcy Code. The US Federal Trade Commission (FTC) intervened to enjoin the sale.⁴⁴ Eventually, a settlement was reached and the sale was permitted on the condition that the data was to be sold only ‘in connection with other corporate assets to a buyer in a related market that would continue the business and, additionally, with a provision of notice and ability for individual consumers to opt out.’⁴⁵ The additional action of the State Attorneys General added the condition that there was to be an opt-in consent mechanism for the sale to be legally permissible. The cumbersome burdens engendered the destruction of the data rather than the sale.

Post-*Toysmart*, the Bankruptcy Abuse Prevention and Consumer Protection Act was introduced in 2005 to reform the insolvency framework. Section 363(b)(1)(B) was added to the Code in response to

⁴³ Federal Trade Commission, ‘Toysmart.com, LLC, and Toysmart.com, Inc. (timeline item) – July 21, 2000’ (21 July 2000) <<https://www.ftc.gov/legal-library/browse/cases-proceedings/toysmartcom-llc-toysmartcom-inc-timeline-item-2000-07-21>> accessed 16 June 2025.

⁴⁴ Sushila Chanana, ‘Privacy During Bankruptcy Proceedings: Why It Matters’ (*Farella Braun + Martel*, 5 November 2020) <<https://www.fbm.com/data-analytics/publications/privacy-during-bankruptcy-proceedings-why-it-matters/>> accessed 24 October 2025.

⁴⁵ *ibid.*

the case. It provides that a debtor that had a privacy policy at the time of data collection may not sell or lease Personally Identifiable Information (PII) unless a consumer privacy ombudsman is appointed, or a Bankruptcy Court determines that the sale is consistent with the privacy policy.⁴⁶ However, the barriers to the sale of PII erected by Section 363(b)(1)(B) are extremely flimsy. First, the necessary condition for the applicability of the provision is that the debtor must have had a privacy policy in place when the data was collected. For the debtors that did not have a privacy policy in force, the consumers are left with absolutely no protection.⁴⁷ Second, the standard set by the Code is vague and subjective, as the only requirement is that the sale should ‘not be inconsistent’ with the privacy policy. This allows companies to get around this condition by intentionally enforcing open-ended and broadly worded policies. Third, the role of the consumer privacy ombudsman is only advisory in nature, and not authoritative, giving scope for the courts to override the ombudsman’s opinion when financial interests are at stake.⁴⁸ Fourth, and most notably, Section 363(b)(1)(B) does not create any substantive privacy rights; instead, privacy remains a subject of contract.⁴⁹ This signifies the US approach, whereby data governance is framed in terms of market regulation, such as voluntary adoption of best practices, as opposed to the EU approach of state-market regulation.⁵⁰

⁴⁶ 11 USC s 363(b)(1)(B).

⁴⁷ William McGeeveran, *Privacy and Data Protection Law* (2nd edn, Foundation Press 2023).

⁴⁸ Daniel J Solove and Chris Jay Hoofnagle, ‘A Model Regime of Privacy Protection’ (2006) 2006 U Ill L Rev 357.

⁴⁹ Woodrow Hartzog, ‘The Inadequate, Invaluable Fair Information Practices’ (2017) 76 Md L Rev 952, 984-86.

⁵⁰ Guay and Birch (n 40).

Even these limited safeguards have been consistently undermined by the Bankruptcy Courts in two ways. For one, the courts have steadily interpreted ambiguous privacy policy provisions in a manner to allow for the sale of PII without the appointment of an ombudsman.⁵¹ The other, courts have avoided the appointment of the ombudsman by imposing on the purchaser the same conditions as in the debtor's privacy policy, thus adopting a 'no harm, no foul' policy.⁵²

The *RadioShack case* in 2015 highlighted the inadequacies of Section 363(b)(1)(B) in protecting PII. The application of the section was triggered because RadioShack had a privacy policy that asserted that the customer data would not be sold or shared with third parties. However, when the company filed for Chapter 11 Bankruptcy, it proposed to sell its customer database as one of its most valuable assets. This was objected to by the FTC and the State Attorneys General, and a court-approved settlement was reached with the conditions that data only be sold to another retailer, the purchaser abide by the original privacy policy, customers be given an opt-out option, and certain sensitive data be excluded.⁵³ Though the conditions imposed could be perceived as onerous, the fact that the sale was permitted despite an explicit promise otherwise demonstrates the contractual nature of privacy rights in the US, and is a testament to their susceptibility to renegotiation and re-interpretation.⁵⁴

⁵¹ Love (n 5).

⁵² *ibid*.

⁵³ *In re RadioShack Corp*, No 15-10197 (Bank D Del 2015).

⁵⁴ Asher Kalman, 'Data Privacy In Bankruptcy: Toward A Deus Ex Machina' (*Columbia Business Law Review*, 26 March 2021) <<https://journals.library.columbia.edu/index.php/CBLR/announcement/view/394>> accessed 24 October 2025.

Thus, in the US context, the financial interests of the various stakeholders, such as the debtor and the purchaser, are sought to be tempered by a relatively weak right to privacy and data protection. However, data being cast in the position of a pecuniary and monetizable asset, the economic benefits arising from the commercialisation of personal data achieve a slight prioritisation. Further, data protection is enabled through a market-based regulation, and post hoc correction of perceived market failures that reinforce the nature of privacy rights as contractual rather than fundamental.⁵⁵

IV. WAY FORWARD FOR INDIA

In India, the tension between the insolvency regime and the privacy regime is articulated in terms of the constitutional and statutory right to privacy, and the mandate of the I&B Code, which requires the maximization of the value of the debtor's assets. This paper proposes the resolution of this tension through the conceptualisation of a hybrid framework that is grounded in an *ex-ante* statutory mechanism as observed in the EU, while also incorporating procedural flexibility that allows for the timely conclusion of the CIRP, preserving the commercial value of data as practised in the US. Such a framework balances the competing considerations of privacy and value-maximisation without compromising either, and passes the three-fold test laid down in the *Puttaswamy* judgement.⁵⁶

The challenge to the Indian legal system comprises the institutionalisation of both values, privacy and value-maximization,

⁵⁵ Guay and Birch (n 40).

⁵⁶ *Puttaswamy* (n 6).

without one overshadowing the other. The significance of privacy was established in the *Puttaswamy case*, where the Supreme Court recognised the right to privacy as encompassed within the constitutional right to life and liberty. Subsequently, the protection of personal data was mechanised in the DPDP Act. The underlying principles of the constitutional guarantee and the DPDP Act are the dignity and autonomy of the individual in decisions relating to personal information. Notably, the DPDP Act is strikingly similar to the GDPR in the EU, though modified for the Indian context. Firstly, the principle of purpose limitation has been codified in Section 6 of the Act.⁵⁷ However, it is not as rigorously entrenched as in the GDPR, as evidenced by the broad legitimate uses clause⁵⁸ and the statutory exemptions where the principle may be bypassed.⁵⁹ Secondly, the condition that ‘consent’ shall be ‘free, specific, informed, unconditional and unambiguous with a clear affirmative action’ employs similar phraseology as the GDPR, signifying that consent requires some positive or overt act by the Data Principal.⁶⁰ These indicia point to the conclusion that the legislative intention in the DPDP Act was to provide substantive privacy rights that reflect their fundamental, rather than contractual character.

The legislative intent behind the I&B Code, on the other hand, is geared towards maximizing the value of the corporate debtor’s assets and resolving the insolvency within strict deadlines. The Code deals with the central problems arising in an economy, that is, the problem of creating availability of credit, the problem of efficient resource utilisation, and the

⁵⁷ DPDPA 2023, s 6.

⁵⁸ DPDPA 2023, s 7.

⁵⁹ DPDPA 2023, s 17.

⁶⁰ DPDPA 2023, s 6.

problem of encouraging entrepreneurship.⁶¹ Though the I&B Code is not a law for recovery,⁶² its attempt to maximize returns for creditors strengthens creditors' confidence, increasing credit availability in the economy. Further, by putting in place a structure for the direction of underutilised resources to more efficient uses through reorganisation or liquidation, the I&B Code displays an underlying acknowledgement of the scarcity of resources in an economy.⁶³ The Code also provides avenues for easy exit from the market for honest entrepreneurs, thereby shielding them from the adverse effects of economic failure, and in turn, creating an environment conducive to entrepreneurship.⁶⁴ This is in line with the economic pragmatism adopted by the US, where the flexibility offered by the procedural mechanisms in the Bankruptcy Code contributes to larger socioeconomic benefits.

Thus, both the I&B Code and the DPDP Act were enacted with distinct objectives that must be preserved and given effect to. This paper envisages their harmonious construction through a tiered approach at the intersection of insolvency and privacy. The classification of data into three tiers – sensitive personal data, personal data with commercial value, de-identified data – allows data protection and monetisation to proceed from a starting point that recognises the nuances within the broad category of 'data', and ensures proportional treatment of each category based on its nature and sensitivity.

⁶¹ M S Sahoo and Anuradha Guru, 'Indian Insolvency Law' (2020) 45 *Vikalpa: The Journal for Decision Makers* 69.

⁶² *Swiss Ribbons (P) Ltd v Union of India* [2019] 4 SCC 17.

⁶³ Sahoo and Guru (n 63).

⁶⁴ *ibid.*

The first-tier deals with ‘sensitive personal data’, which requires greater protection as transmission can pose a higher risk to the privacy of the concerned individuals. In the EU, sensitive data is referred to as ‘special categories of personal data’, and includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.⁶⁵ The processing of such data is under a default prohibition under the GDPR, unless a specific exemption is applicable.⁶⁶ In insolvency contexts, the transfer of special categories of personal data is either heavily regulated or entirely blocked. In the US, there is no single definition of sensitive data owing to the lack of a federal legislation on data privacy, however, the California Consumer Privacy Act, which is the most comprehensive US data protection legislation, includes within the ambit of ‘sensitive personal information’ state-authorized identifiers such as social security numbers, account log-ins and other financial information, geolocation, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership, the contents of private communication, genetic data, and neural data.⁶⁷ These are generally allowed to be processed depending on the state, unless the consumer invokes the opt-out option. Transfer of such data during insolvency is permissible if some mitigative measures, such as an option to object, are provided to consumers. Drawing from these illustrative definitions of sensitive personal data, the Indian legal system should isolate some kinds of data as requiring more scrutiny

⁶⁵ GDPR, art 9(1).

⁶⁶ GDPR, art 9(2).

⁶⁷ Cal Civ Code s 1798.140(ae).

when it comes to asset sales in the resolution plan or liquidation proposal. Reaching a middle ground between the EU rigidity and the US permissiveness, India should strive to set in place certain protective mechanisms, such as the requirement of explicit opt-in consent by consumers, and a mandatory privacy impact assessment.

The second tier comprises ‘personal data with commercial value’ such as purchase history, browsing data, frequent flyer records (as in the case of *Jet Airways*), which are collected during the ordinary course of business. Second-tier data may be transferred during asset sales as part of a resolution plan or liquidation proposal; however, such a transfer must be contingent on safeguards such as anonymisation of data where possible, and a mandatory provision of notice and opportunity to opt-out both pre-transfer and post-transfer. Arriving at a balance between privacy and value-maximisation legitimately corresponds with the larger socioeconomic benefits to creditors, debtors, and consumers derived from such transfers without negating the consumers’ dignity and autonomy.

The third tier refers to ‘de-identified data’ that are part of large analytic and anonymised data sets. The defining characteristic of this kind of data is that identification is not reasonably possible or foreseeable. As they pose no risks to individuals’ privacy rights, these may be freely transferred and monetised during the course of the CIRP.

The operationalisation of this three-tier model would require coordination between existing authorities under the insolvency and privacy regimes in a time-bound manner. First, the resolution professional must identify and classify the data in the corporate debtor’s possession with reference to the three tiers outlined. Second, the

resolution professional with the oversight of the Data Protection Board of India must conduct a privacy impact assessment for any proposed data transfers. Third, at the time of plan approval, the NCLT must ensure the attachment of a privacy compliance certificate which verifies that the plan does not infringe on the privacy rights of the consumers. Fourth, the consumers must then be notified regarding any transfers pertinent to them and be provided with an opt-out window so that the process of data transfer is consensual.

A comprehensive legislation that adopts the tiered approach proposed in this paper not only harmonises the privacy and insolvency regimes, but also passes the three-fold test of the *Puttaswamy case*.⁶⁸ Firstly, it postulates the existence of a law. Since privacy cannot be infringed upon through executive action alone, the Parliament must pass legislation that addresses the legal lacuna regarding privacy rights during the insolvency of the data fiduciary/corporate debtor. Secondly, it fulfils a need in terms of a legitimate state aim. Privacy of consumers during the CIRP would be curtailed not arbitrarily, but in pursuance of the legitimate state aims as stated in the preamble of the I&B Code. Thirdly, it embodies the principle of proportionality in that there is a rational nexus between the object sought to be achieved (maximisation of asset value) and the means adopted to achieve it (an intricate three-tiered model that incorporates suitable principles from the EU and the US jurisdictions). Thus, the hybrid approach based on the experience of foreign jurisdictions would effectively ease the tensions between the I&B Code and the DPDP Act.

⁶⁸ *Puttaswamy* (n 6).

V. CONCLUSION

This paper brings to focus the legal vacuum created by the isolated functioning of the I&B Code and the DPDP Act. Though they are comprehensive legislations in the fields of insolvency and privacy, respectively, neither provides clear or unambiguous instructions on how to operate at the intersections of insolvency and privacy, particularly in a situation where a data fiduciary becomes a corporate debtor. The lack of any regulations at this juncture permits structural disregard for the data principals' privacy rights through the transmission of data as part of asset sales in a resolution plan or liquidation proposal.

In the age of digitalisation, we can no longer rely on only executive or judicial action to fill this gap. The detached operation of the I&B Code and the DPDP Act, and the lacunae consequently created, must be addressed through legislative action. In lieu of this, the approaches in foreign jurisdictions were presented as possible alternatives for the silence in India. In the EU, the GDPR, being the supranational privacy law, took precedence over national insolvency laws. It imposed normatively superior but practically unfeasible restrictions on the processing of data. Such conditions adequately protected the data subjects' privacy rights, but imposed hardship on the debtor companies, leading to the devaluation of data. However, the ex ante formulation of regulations created certainty and predictability in the legal system. In contrast, the US did not have a federal data privacy law; however, the question of the sale of data during insolvency was codified in the federal Bankruptcy Code. Though it created new and dedicated institutions such as the Consumer Privacy Ombudsman, the law fails to adequately address the privacy concerns due to its procedural approach being that

of *post hoc* correction of market regulation of data protection. Yet, the paper identified procedural flexibility and economic maximisation of value as the distinct advantages of the US model.

In the final analysis, the paper proposed a three-tiered approach that treated distinct classes of data differently on the basis of their sensitivity and identifiability. Such an approach borrows principles from both the EU and the US laws, and optimally reimagines them to suit the Indian context. In doing so, it harmonises the I&B Code and the DPDP Act while giving effect to the legislative intent and objects of both legislations. The paper also demonstrated that legislation to mechanise the three-tiered approach would pass the three-fold test of constitutionality laid down in the *Puttaswamy* judgement. Thus, the critical blind spot identified in the insolvency and privacy regimes of India can be hammered away through the incorporation of these pragmatic recommendations into the law.