INSOLVENCY AND THE VALUE OF DATA: RECONCILING ASSET MAXIMIZATION UNDER THE IBC WITH DATA PROTECTION UNDER THE DPDP ACT

Mohammad Farhat, Prestige Institute of Management & Research, Department of Law, Indore

ABSTRACT

In today's digital world, corporate insolvency has reached beyond physical assets to data including personal, transactional, and algorithmic data as a primary source of enterprise value. Notwithstanding this paradigm shift, the Indian Insolvency and Bankruptcy Code (IBC), 2016, and the Digital Personal Data Protection (DPDP) Act, 2023[1], do not have a coordinated framework to regulate the valuation, management, and transmission of data assets in insolvency. This paper critically analyzes the existing legal vacuum, contrasts best global practices, and suggests an integrated legal framework to achieve both asset maximization and privacy in India's insolvency regime.

With the increasing reliance of businesses on digital ecosystems, in contemporary cases of bankruptcy, what could well be the most important element within the corporation is not real estate, equipment, or inventory but the information ecosystem within which the business operates. Behavioral data of customers, algorithms for recommending products or services, transaction history, libraries of source code, logistics knowledge, and predictive tools are all part of the bedrock of business continuity. However, information assets differ fundamentally from other types of property in that they are replicable, regulated by law, and associated with fundamental rights.

Keywords: Insolvency and Bankruptcy Code (IBC), Digital Personal Data Protection Act (DPDP), Data as Asset, Corporate Insolvency, Data Valuation, Asset Maximization, Privacy Rights, Resolution Professionals, Digital Assets, Data Transfer, Insolvency Law, Information Privacy, India, Cross-Border Insolvency, Regulatory Harmonization.

[1] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016 (India); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

1. *Introduction:*

India's digital revolution has transformed the character of business assets. Databases, intellectual algorithms, and consumer data now constitute the foundation of business value and decision making. Insolvency of firms carries with it these digital assets unique legal, ethical, and economic challenges. India's regulatory framework still has no clear, actionable approach to dealing with data in distress, exposing both asset undervaluation and privacy infringement. This paper fills these voids and suggests actionable policy reform recommendations.

The matter is especially relevant for India given the growing emergence of digital businesses, financial technology firms, healthcare technology providers, education technology companies, logistics aggregators, and software-as-a-service ventures. These enterprises might grow based on network effects instead of asset growth strategies. As such, their market valuation might even exceed their book valuation since markets take into account the monetization of their information system in the future. Therefore, when such corporations become insolvent, the typical accounting methods will fail to determine the real property of value contained within the informational assets.

Moreover, the data should not be considered a typical commodity. Personal data could be related to issues concerning dignity, autonomy, surveillance, informational self-determination, and cyber security. Given that the Indian Supreme Court has ruled that privacy is a fundamental right in Justice K.S. Puttaswamy v. Union of India, the transfer of personal data in insolvency cases needs to be assessed under this constitutional framework.[2]

2. *Data's Evolution and Importance as an Asset:*

- ***Data as the New "Oil" of Contemporary Economies[3]***

As the world economy goes digital, corporations have shifted from being majorly based on physical assets like machinery, infrastructure, and inventory, to establishing competitive advantage through intangibles. Databases of millions of users, personal or transactional

---

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, recognizing privacy as a fundamental right under Article 21 of the Constitution of India.

[3] The phrase "data is the new oil" is widely attributed to British mathematician Clive Humby in 2006, highlighting the value of raw data when refined.

information can be used for precise marketing, retaining customers, and forward looking analytics. Algorithms and specialized software run fintech platforms, online marketplaces, and service delivery models, providing firms with unique operating leverage.

The economic significance is highlighted by blockbuster bankruptcies and acquisitions in which the worth of user data, customer relationship management databases, or intellectual property eclipses the worth of hard assets. For instance, high-profile tech industry acquisitions frequently list customer lists and behavior information as key drivers of acquisitions.[4]

- ***Monetizable Potential and Corporate Valuations***

From a valuation point of view, information is now among the most important assets of a company included in financial reports and due diligence procedures. Sales or licensing of databases provide financially distressed companies with a means to raise much-needed liquidity for their creditors. Industries from retail and e-commerce to financial services and health tech depend on data liquidity and portability.

Data can potentially be valuable in many ways, such as its direct sale or license, increased efficiency, reduction of the costs of acquisition by focused marketing, lower levels of fraud, better customer retention, and even through its derivatives. As such, insolvency experts who fail to capitalize on this aspect run the risk of failing their statutory duties.[5]

But this monetization converges with primary legal issues like data protection, user consent, and cyber resilience. Of particular interest, in insolvency, the conflict between maximizing value for creditors and consideration of privacy/contractual obligations is at the forefront.[6]

- ***International Recognition of Data as an Asset***

Worldwide, the GDPR (European Union), the California Consumer Privacy Act (United States), and ICO guidelines (United Kingdom) increasingly acknowledge both the

[4] Example: Facebook's acquisition of WhatsApp in 2014 valued user base and metadata over tangible assets. See: SEC Filings, Facebook Inc., 2014.
[5] Insolvency and Bankruptcy Code, 2016, Section 25(2)(h), requiring the Resolution Professional to maximize the value of assets of the corporate debtor.
[6] See GDPR Recital 39 and Articles 5–6 for principles regarding lawful data processing and limitations.

economic and legal aspects of data as an asset, particularly where ownership or control is transferred through insolvency or merger.

It is now increasingly apparent that issues relating to accounting and corporate governance have taken on the additional dimension of whether data assets created internally merit greater recognition when it comes to valuing businesses. The accounting literature may still lag behind, but the business world already recognizes and values such assets.[7]

- ***Nature of Data as Property***

The first major problem lies in whether data is "owned" in the conventional sense. Unlike land or equipment, data does not depreciate through usage since it can be duplicated an infinite number of times. There are multiple concurrent owners of the same set of data—the data principle, the collecting company, processors, servers, and the regulator. Therefore, data must be considered as a combination of rights pertaining to control, access, right to process data, contractual right, and technological ability.

This difference is important from the point of view of bankruptcy. If data is seen as regular proprietary property, it can easily be transferred in order to derive maximum benefit out of it. If, however, it is viewed as relational data subject to ongoing rights, it becomes conditional.

3. *Gaps in the Indian Legal Framework:*

The Insolvency and Bankruptcy Code (IBC), 2016: Silence Areas

Whereas the IBC's purpose is to facilitate time-bound resolution and optimal value realization of all stakeholders, it does not classify digital assets like data, algorithms, or consumer analytics in their own selves as "assets" per se. Such exclusion leads to ambiguity for insolvency professionals:

- Asset Identification: Must datasets, trade secrets, proprietary algorithms, or user data form part of asset registers and valuation reports.

[7] OECD, Data-Driven Innovation: Big Data for Growth and Well-Being (OECD Publishing, 2015)

- Procedural Clarity: In the absence of clear procedures to deal with and sell such assets, Resolution Professionals (RPs) will find it difficult to both satisfy corporate law and the new data protection needs.

The absence of legislative directions impedes creditor recoveries, creates litigation opportunities, and causes uncertainty among potential buyers.

Also, the requirements of Sections 18 and 25 of the IBC necessitate that the IRP and RP gain control of the assets of the debtor. However, in case of companies with digital operations, the control might require that the RP has the login credentials and encryption keys, details of the cloud contracts, sources of the codes, API structure, and cybersecurity measures, which are not explicitly mentioned in the statute.[8]

The Digital Personal Data Protection (DPDP) Act, 2023: Unresolved Privacy Tensions

The DPDP Act, enacted for safeguarding individual autonomy, forbids processing or transferring information without definite, specific, informed consent. In the event of insolvency:

- Transfer Limitations: The acquirer of an insolvent firm's property cannot inherit the right to personal data automatically unless original data principals (users) give explicit consent or unless the data is anonymized.

- Purpose Limitation: Data employed for a single commercial purpose cannot, according to law, be reused for another purpose unless new consent is obtained.

In contrast to the GDPR's detailed insolvency carve-outs, the DPDP Act is mum on the status and acceptable treatment of data during bankruptcies, creating tensions between insolvency and privacy regulators and halting distressed sales.

The Policy and Enforcement Vacuum

There is no guidance from the Insolvency and Bankruptcy Board of India (IBBI) or the

[8] Insolvency and Bankruptcy Code, 2016, Sections 18 and 25 dealing with control, custody, preservation and management of assets.

Data Protection Board (DPB) on:

- Enforcement of privacy during asset sales
- Allocation of liability (in case of data breach following data transfer)
- Secure deletion, anonymization, or ongoing storage of data following sale or liquidation

This absence of coordination inhibits innovation in insolvency practice, puts privacy at risk, and could ultimately lead to decreased market confidence in India's insolvency resolution process.

Constitutional Dimensions

India's privacy rights have both a legal and a constitutional aspect. Informational privacy was found to be an essential component of dignity and liberty guaranteed under Article 21 in the landmark case of Puttaswamy. Hence, the statutory and administrative provisions that permit the transfer of personal data in case of insolvency shall have to comply with legality, necessity, and proportionality principles.[9]

This implies that irrespective of whether a data sale is economically sensible, the state shall not authorize an indiscriminate transfer when other options that are less intrusive are available, including anonymization, selective licensing, segmented transfers, and renewed consent mechanisms.

4. The Regulatory Tension: Asset Maximization vs. Privacy:

Valuation Dilemmas

How would an RP appropriately value datasets with millions of user records where their transfer or use is unclear according to the law? Classic valuation models (projected cash flows or comparable transactions) could fail to depict the actual, enforceable value if there are legal hurdles to their transfer.

The data set might prove to be a financially rewarding proposition on paper, but could be

[9] Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353; proportionality doctrine later affirmed in Puttaswamy.

compromised when it comes to commercial viability due to limited consent, old data, or lack of cyber security that leaves the buyer open to legal action.[10]

Consent, Repurposing, and Third-Party Rights

In highly privacy-oriented jurisdictions, courts have halted transfer of user/customer databases where consumer notice or consent is not present. India is similarly at risk. Also, transfer to a new corporation or investor might amount to a change of purpose and necessitate either new data principal consent or rock-solid anonymization.

Data Breaches and Legal Exposure

If the data is transmitted or sold in contravention of the DPDP Act or without effective cybersecurity safeguards, the party, be it the RP, CoC, or the end buyer, may suffer liabilities from fines by the regulator to civil lawsuits.[11] Such data breaches at Indian entities in recent high-profile cases highlight the seriousness of such risks during transition or change in corporate control.

Competing Objectives

Therefore, the seeming conflict: creditors' value maximization (the IBC's aim) and strict user privacy and individual rights protection (the DPDP Act's philosophy). Not resolved, such conflict can impede insolvency proceedings, lower potential asset value (from legal complications or data transfer unability), and erode public confidence in the system.

5. *Comparative Perspectives: Lessons from Global Jurisdictions:*

European Union (EU): GDPR Protection in Insolvency

The GDPR has explicitly banned the transfer of personal data, except where the transfer accords with its central principles.[12] Insolvency practitioners are required to:

---

[10] ISO/IEC 27001 Information Security Management Standards are frequently used benchmarks in due diligence for data-intensive transactions.
[11] Under DPDP Act, 2023, Sections 33–36 outline penalties for breach, with fines up to ₹250 crore for failure to protect personal data.
[12] General Data Protection Regulation (EU) 2016/679, Article 6 (Lawfulness of processing) and Article 44 (Transfers).

- Carry out Data Protection Impact Assessments (DPIA) before selling assets
- Notify and where necessary, obtain consent from the data subjects
- Comply with the same privacy protection by the acquirer
- Direct erasure in case data transfer is not permissible

Failures have led to regulatory intervention, as in the "In re: Cambridge Analytica" situation, which resulted in data wiping out instead of transfer.[13]

United States: FTC Oversight and Precedent-Setting Cases

- During Toysmart.com's bankruptcy, the FTC protested against the sale of the customer database because it was against Toysmart's expressed privacy policy of "no sale or transfer."[14]
- Court orders and settlements needed data anonymization or deletion, unless customers were informed and given the option to opt-out.

US bankruptcy courts usually weigh economic and ethical issues against each other, referring to privacy policies, consumer sentiment, and regulatory advice before sanctioning sales of data.

United Kingdom: ICO Guidance for Insolvency Practitioners

The UK's Information Commissioner's Office (ICO) requires insolvency practitioners to[15]:

- Comply with Data Protection Act principles throughout the resolution process
- Complete a Data Protection Impact Assessment when moving personal data
- Notify data subjects of any substantial change in data controller status

[13] UK Information Commissioner's Office investigation into Cambridge Analytica and related entities emphasized deletion and lawful processing obligations.
[14] FTC v. Toysmart.com, No. 00-11341-RGS (D. Mass. 2000).
[15] Information Commissioner's Office (UK), "Insolvency Practitioners and the UK GDPR," Guidance Note, 2020.

- Make buyers able to meet privacy commitments made to data subjects

Fines and civil penalties enforce these requirements.

Other Common Law and Civil Law Nations

Jurisdictions such as Australia and Canada are developing comparable standards, more requiring distinct regulatory clearances, customer notice procedures, and continued privacy safeguards throughout and following insolvency transfers.

Cross Border Insolvency and Data Localization

It is common practice among present-day companies to maintain user data from India in cloud servers worldwide. In case such a company faces insolvency proceedings in various jurisdictions, a complex situation emerges as to which court would be competent to take charge of the data, what privacy laws would apply, and whether foreign administrators can have access to Indian personal data.

The process by which India slowly becomes acquainted with international insolvency proceedings principles through the UNCITRAL Model Law requires parallel data protection measures as well. Without such, India's citizens' data might become susceptible to divergent legal frameworks.[16]

6. *Indian Law and Recent Developments:*

Absence of Direct Precedents

Indian courts have as yet not fully broached the collision of insolvency and data protection. Nonetheless, NCLT orders in situations like Jet Airways and DHFL have brought to the forefront the need to safeguard stakeholder interests, employees and customers alike.

As digital bankruptcies become more common, there will inevitably be cases involving issues relating to cloud server access, software escrow rights, data migration, and liability from previous breaches. Early legal precedent will be particularly important and must be

[16] UNCITRAL Model Law on Cross-Border Insolvency, 1997, adopted in multiple jurisdictions as a framework for recognition of foreign insolvency proceedings.

driven by clear legal theory and not merely practical considerations.[17]

Notable Sectoral Guidelines

Some regulators (RBI, SEBI, IRDAI) have made sector-specific guidelines for data storage, retention, and transfer (specifically related to sensitive financial information) across corporate changeovers.[18] Yet these guidelines fall short of setting out exhaustive rules applicable to insolvency.

Emerging Disputes

There are reported rising disputes in bankruptcy sales related to tech firms or NBFCs with buyers, RPs, and privacy experts challenging terms of data asset transfers and related liability.

7. *Stakeholder Analysis: Who Benefits, Who Loses?*

Creditors

Optimized asset realization can rely on the legal, effective transfer of value-added information that supports continuing operations, makes the distressed unicorn or start-up more attractive, and attracts a broader base of bidders.

Resolution Professionals

RPs bear responsibility for due diligence, adherence to the law, and safe handling of data in a fluid, frequently litigious process. Ambiguity of rules leaves them subject to substantial liability.[19]

Buyers

Investors have to balance the ultimate use and legality of purchased information with the threat of investigation, fines, or negative publicity if information was passed on in violation

---

[17] Swiss Ribbons Pvt. Ltd. v. Union of India, (2019) 4 SCC 17, affirming the objective of value maximization and revival under the IBC.

[18] For example, RBI Master Direction on IT Framework for NBFCs (2017); SEBI Cybersecurity Framework Circular (2019).

[19] Insolvency and Bankruptcy Board of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016, prescribing duties of diligence and disclosures.

of privacy law.

Data Principals (Consumers/Users)

Piped into stake are their constitutional and statutory rights of privacy, informed consent, and data security rights that can be inadvertently or maliciously eroded in uncontrolled sale of assets.

Regulatory Bodies

Both DPB and IBBI are interested in safeguarding their spheres. In the absence of inter-agency coordination, turf battles or regulatory arbitrage can result.

8. *Suggestions towards a Harmonized Indian Framework:*

1. Statutory Recognition of Data as an Asset

Reform the IBC to include digital assets and data as asset classes that need protection. Define algorithms, data, and proprietary software as asset registers.

Advantages: Provides RPs with clarity; promotes professional standard of valuation; ensures potential for maximum recovery for creditors.

2. Data Valuation Standards

Task regulatory authorities, e.g., IBBI with market professionals and data science specialists as consultees, to formulate sector-specific guidelines for measuring economic value of data.

Include:

- Revenue models as a function of data usage
- Market comparables in the case of sales of similar assets
- Legal enforceability discounts where transfer is impaired
- Evaluation of quality, completeness, and lawfulness of data sets

3. Comprehensive Consent Management

RPs have to set down protocols for

- Customer notification on the initiation of insolvency
- Securing new consent for any planned new uses or transfers of data
- Mechanisms for opt-out, correction of data, or erasure if data principals withhold consent

4. Privacy Impact Assessments (PIAs)

Make PIAs mandatory prior to transferring data in insolvency cases, assessing:

- Risks of re-identification or misuse
- Compliance with DPDP and applicable sectoral guidelines
- Data minimization and anonymization measures

5. Inter-Regulator Coordination and Advisory Committees

Institutionalize a permanent task force between DPB (and sectoral regulators) and IBBI to:

- Publish joint guidelines or FAQ bulletins for RPs and CoC
- Approve and review major data asset transfers
- Monitor post-sale implementation

6. Transparency and Disclosure

Require RPs to disclose clearly to bidders the quantum, quality, and legal encumbrance relating to data assets.[20]

Potential buyers should be fully informed about ongoing privacy requirements, reporting

[20] Transparent disclosure norms improve bid efficiency and price discovery in distressed asset markets.

obligations, and the necessity of sustained compliance after acquisition.

7. Judicial Clarification

Pursue development of model guidelines for NCLT benches to balance weighing IBC priorities alongside privacy rights.

Establish case law drawing on international best practice, note for instance the US bankruptcy courts' approach or the ICO's DPA16 guidance.

8. Model Clauses and Standardised Contracts

Provide model contract templates with:

- Buyer's post-sale privacy responsibilities
- Liability clauses for pre- and post-transfer breaches
- Data deletion/anonymization procedures for non-transferable data

9. Education and Capacity Building

Create training modules and certification for RPs, asset valuers, and lawyers on management of digital assets, risks of privacy, and international standards.[21]

Public education campaigns to educate data principals regarding rights and processes in insolvency situations.

10. Periodic Review and Feedback Loops

Establish a system of periodic review with feedback from stakeholders for tighter regulations and adjustments according to changing technology, market, and privacy risks.

11. Establishment of Digital Asset Valuation Experts

Pools of experts comprising financial, cybersecurity, and data governance professionals

[21] Suggested in IBBI's Discussion Paper on Resolution Professionals' Role, 2022, and echoed in public consultations.

may help RPs.

12. Separation of Personal and Non-Personal Information

All information cannot be treated equally. Business KPIs and anonymous analyses may have greater mobility compared to personal details.

13. Regulatory Sandbox

IBBI and DPB can establish a regulatory sandbox to test optimal practices in difficult digital insolvency cases.

14. Competition Analysis

In cases where dominant platforms target their struggling counterparts only for information consolidation, the Competition Commission of India must investigate any anti-competitive behavior.[22]

9. ***Suggested Legal Reforms: Roadmap for Stronger Implementation:***

- IBC Amendment: Update Section 3 of IBC to clearly define assets to include digital property and data, giving due process and safeguards.[23]
- Regulations under DPDP: Enact new regulations under DPDP Act specifically covering insolvency situations, with well-defined processes of consent, notice, and transfer.
- Harmonized Protocols: Release harmonized guidelines for RPs outlining brick-to-brick asset management, right up to last liquidation or post-sale transition.
- Template Contract Clauses: Provide government officials with vetted contract templates to reduce disputes and post-sale litigation.
- Capacity Building: Create continuing professional education courses to RPs that keep pace with international data protection and asset valuation trends.

---

[22] Competition Act, 2002, Sections 5 and 6 regulate combinations that may cause appreciable adverse effect on competition.

[23] Section 3 of IBC currently defines "assets" without express mention of data; see IBC, 2016, 3(2).

10. Conclusion

The future insolvency landscape will be characterized not only by physical asset recovery, but by the lawful, ethical, and innovative management of digital assets, personal and commercial data. India is at the turning point: either it persists with ad hoc arrangements, inviting lost opportunities and public suspicion, or it pioneers the world by aligning value maximization with data privacy in insolvency.

An insolvency regime in the modern world cannot continue to be based on an industrial-age understanding of assets, in an era where the economy itself has become informational. Information is productive capital, reputational capital, and strategic capital. It is also an expression of human personality, if associated with identifiable persons.

If India succeeds in reconciling the IBC with DPDP, then it will be able to establish a model for restructurings in the information age that takes credit risks seriously while respecting the dignity of its citizens, that promotes investments but not at the expense of fundamental freedoms, and makes insolvency more about renewal than liquidation.[24]

[24] Committee of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta, (2020) 8 SCC 531, emphasizing revival and value maximization as core IBC objectives.

REFERENCES:

Statutes / Legislation

1. Insolvency and Bankruptcy Code, No. 31 of 2016, India Code (2016).

2. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

3. Competition Act, No. 12 of 2003, India Code (2003).

4. Information Technology Act, No. 21 of 2000, India Code (2000).

Cases (India)

5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

6. *Swiss Ribbons Pvt. Ltd. v. Union of India*, (2019) 4 S.C.C. 17 (India).

7. *Committee of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta*, (2020) 8 S.C.C. 531 (India).

8. *Jet Airways (India) Ltd. v. State Bank of India*, CP (IB)-2205/MB/2019 (NCLT Mumbai Bench).

9. *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 S.C.C. 353 (India).

Foreign Cases

10. *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. 2000).

International / Foreign Regulations

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

12. United Nations Commission on International Trade Law (UNCITRAL), Model Law on Cross-Border Insolvency (1997).

13. California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (2018).

Government / Regulatory Materials

14. Reserve Bank of India, Master Direction – Information Technology Framework for the NBFC Sector (Feb. 8, 2017).

15. Securities and Exchange Board of India, Cyber Security and Cyber Resilience Framework for Stock Brokers and Depository Participants, Circular No. SEBI/HO/MIRSD/DOP/CIR/P/2019/146 (Dec. 19, 2019).

16. Information Commissioner's Office (UK), Insolvency Practitioners and the UK GDPR: Regulatory Guidance (2020).

17. Insolvency and Bankruptcy Board of India, Discussion Paper on Strengthening the Role of Resolution Professionals (2022).