

THE INSOLVENCY–PRIVACY CONFLICT: REGULATING THE TRANSFER OF PERSONAL DATA DURING CORPORATE INSOLVENCY IN INDIA

by

JEYAN VISHNU VARDAN

ABSTRACT

When a company enters insolvency, its customer databases, employee records and user profiles often become some of its most valuable assets. Indian insolvency law treats these assets like any other property to be preserved, shared with bidders and, if needed, sold. Privacy law takes a different view. It treats personal data as something that belongs to the individual and may be used only for a lawful purpose. This article examines how the Insolvency and Bankruptcy Code, 2016 and the Digital Personal Data Protection Act, 2023 collide when personal data must be transferred during a corporate insolvency. It argues that the Code is silent on data protection, that the 2023 Act does not expressly provide for insolvency, and that this gap exposes data principals to avoidable harm. Drawing on Indian constitutional jurisprudence and comparative experience from the United States and the European Union, the article proposes practical reforms, including a data protection duty for insolvency professionals, staged disclosure of data, and a bar on sales that ignore the purpose for which the data was collected.

Keywords: Corporate Insolvency; Personal Data; Data Protection; Right to Privacy; Resolution Professional; Liquidation; India

I. Introduction

Companies today run on data. A retail platform holds the purchase history of millions of customers, a hospital chain holds medical files, and a fintech lender holds financial records and identity documents. When such a business fails, this information does not disappear. It sits inside the company as an asset, and the people who manage the insolvency must decide what to do with it.

The Insolvency and Bankruptcy Code, 2016 (the Code) was enacted to bring time bound and value maximising resolution to distressed companies.¹ Its focus is on creditors, going concern

¹The Insolvency and Bankruptcy Code, 2016, No. 31 of 2016, §§ 17, 18, 20, India Code (2016).

value and speedy outcomes. The Digital Personal Data Protection Act, 2023 (the DPDP Act) was enacted with a very different focus, namely the protection of the individual whose data is processed.² The Supreme Court had already laid the ground for this in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where it held that privacy is a fundamental right under the Constitution.³

The two laws were drafted for different purposes and neither one speaks to the other. This creates a real problem. A resolution professional may need to share customer data with prospective bidders, and a liquidator may wish to sell a database to recover money for creditors. The individuals whose data is involved never dealt with the bidder or the buyer. They shared their information with a company they chose, for a purpose they understood.

This article asks how personal data should be handled when a company in India goes through insolvency. Part II explains why data has become an insolvency asset. Part III sets out the legal framework. Part IV analyses the conflict. Part V looks at how the United States and the European Union deal with the issue. Part VI offers reform proposals, and Part VII concludes.

II. Personal Data as an Insolvency Asset

The Bankruptcy Law Reforms Committee, whose report shaped the Code, saw insolvency as a way to preserve the value of a business and to balance the interests of all stakeholders.⁴ The Supreme Court has repeatedly described the Code in similar terms. In *Innoventive Industries Ltd. v. ICICI Bank*, the Court explained the Code as a complete scheme for time bound resolution, backed by a moratorium and a change of control over the debtor.⁵ In *Swiss Ribbons Pvt. Ltd. v. Union of India*, the Court upheld the Code and described its objectives as the resolution of distress, the maximisation of asset value and the promotion of credit availability.⁶

The Code gives the interim resolution professional control and custody of the assets of the corporate debtor and the power to manage its operations as a going concern.⁷ A resolution professional must also prepare an information memorandum, and prospective resolution

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

³*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

⁴Bankruptcy Law Reforms Comm., Ministry of Fin., Gov't of India, *The Report of the Bankruptcy Law Reforms Committee* (2015).

⁵*Innoventive Indus. Ltd. v. ICICI Bank*, (2018) 1 S.C.C. 407 (India).

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

⁷Insolvency and Bankruptcy Code, 2016, §§ 18(f), 20.

applicants are entitled to receive relevant information, subject to a confidentiality undertaking.⁸ In liquidation, the liquidator may sell the assets of the corporate debtor, and the Liquidation Process Regulations lay down how such sales are to be run.⁹

None of these provisions mentions personal data. Yet in a modern business, a customer database may be the main reason a bidder shows interest. A going concern sale of a digital business is, in practical terms, often a sale of its data. The difficulty is that the people behind the data are not creditors, are not part of the committee of creditors, and have no voice in the process.

III. The Legal Framework

A. *The Insolvency and Bankruptcy Code, 2016*

The Code is built around a few ideas. Control of the debtor passes to a professional, a moratorium protects the estate, and the committee of creditors decides the future of the business. The Supreme Court has emphasised that the commercial wisdom of the committee is central to this design. In *Committee of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta*, the Court held that courts should not ordinarily interfere with the commercial decisions of the committee, although a plan must still comply with the Code.¹⁰

This focus on creditors explains why privacy has not entered the process. The professional owes duties to the estate and to creditors. No provision of the Code requires the professional to ask whether a data transfer is lawful under another statute. The Code also tells us that a successful resolution plan binds all stakeholders. In *Ghanashyam Mishra and Sons Pvt. Ltd. v. Edelweiss Asset Reconstruction Co.*, the Court held that once a plan is approved, claims not part of it are extinguished, giving the resolution applicant a clean slate.¹¹ That principle is sound for debts. It should not be stretched to suggest that privacy obligations toward individuals can simply be wiped away.

⁸*Id.* § 29; Insolvency & Bankr. Bd. of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016, reg. 36 (India).

⁹Insolvency and Bankruptcy Code, 2016, §§ 35, 36; Insolvency & Bankr. Bd. of India (Liquidation Process) Regulations, 2016, reg. 32 (India).

¹⁰*Comm. of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta*, (2020) 8 S.C.C. 531 (India).

¹¹*Ghanashyam Mishra & Sons Pvt. Ltd. v. Edelweiss Asset Reconstruction Co.*, (2021) 9 S.C.C. 657 (India).

B. The Digital Personal Data Protection Act, 2023

The DPDP Act applies to digital personal data and places obligations on a data fiduciary, which is the entity that decides the purpose and means of processing.¹² The general rule is that personal data may be processed only for a lawful purpose, either with the consent of the individual or for a defined legitimate use.¹³ The individual must be given notice that states the data collected and the purpose of use.¹⁴ The fiduciary must also keep reasonable security safeguards, remain responsible for the data in its possession, and erase data once the purpose is no longer served.¹⁵

The Act contains exemptions in section 17. One of them covers processing necessary for a scheme of compromise, arrangement, merger, amalgamation, demerger or transfer of an undertaking that is approved by a court, tribunal or other competent authority.¹⁶ This looks helpful at first glance, but it does not mention insolvency or liquidation. A resolution plan approved by the adjudicating authority under the Code is not obviously the same thing as a scheme under company law. Reading the exemption to cover insolvency would be a stretch, and an uncertain reading is a poor foundation for sensitive data transfers.

The Act has been brought into operation in stages. The Digital Personal Data Protection Rules, 2025 were notified to give effect to its provisions, with phased commencement.¹⁷ Readers should therefore check the commencement position of each provision when applying the Act.

C. The Earlier Regime and the Constitutional Backdrop

Before the DPDP Act, personal data was protected mainly through section 43A of the Information Technology Act, 2000 and the 2011 Rules on reasonable security practices and sensitive personal data. Those Rules required consent for collecting sensitive data and restricted its disclosure to third parties.¹⁸ The DPDP Act is designed to replace this regime, including by omitting section 43A once the relevant provision comes into force.

¹²Digital Personal Data Protection Act, 2023, § 2.

¹³*Id.* §§ 4, 6, 7.

¹⁴*Id.* § 5.

¹⁵*Id.* § 8.

¹⁶*Id.* § 17(1).

¹⁷The Digital Personal Data Protection Rules, 2025 (India).

¹⁸The Information Technology Act, 2000, No. 21 of 2000, § 43A, India Code (2000); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rr. 5, 6 (India); Digital Personal Data Protection Act, 2023, § 44.

The constitutional position is stronger than either statute. In *Puttaswamy*, the Court recognised informational privacy as part of the right to life and personal liberty.¹⁹ Any state action that limits privacy must satisfy legality, a legitimate aim and proportionality. The Court applied this proportionality approach again in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (the Aadhaar judgment).²⁰ An insolvency process run under the Code, supervised by the National Company Law Tribunal, is a statutory process. A transfer of personal data within it can fairly be tested against these standards.

IV. Analysing the Conflict

A. Purpose Limitation Versus Value Maximisation

The central tension is easy to state. Privacy law says that data collected for one purpose should not be used for another unrelated purpose without fresh consent. Insolvency law says that assets must be used to produce the best return for creditors. A customer who gave her details to buy shoes online did not agree to have that information sold to a stranger for marketing.

This is not a purely theoretical worry. The Justice B.N. Srikrishna Committee, in its report on data protection, stressed that processing should be fair, purpose bound and based on consent, and it identified the weak position of individuals against large data holders.²¹ A sale in insolvency repeats this weakness, because the individual has no bargaining power and often learns of the transfer after it has happened.

B. Who Is Responsible?

A second difficulty is the question of who acts as the data fiduciary once insolvency begins. The corporate debtor remains the legal entity, but management is in the hands of the resolution professional. If a breach occurs during the process, it is unclear whether the debtor, the professional or the bidder must answer for it. The DPDP Act places heavy penalties on fiduciaries for failure to protect data, but it was not written with the insolvency professional in mind.²²

The Code does not help here. It gives the professional wide powers over the assets, but it does not say that these powers are subject to data protection duties. In practice, professionals may

¹⁹*Puttaswamy*, (2017) 10 S.C.C. 1.

²⁰*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India).

²¹Comm. of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

²²Digital Personal Data Protection Act, 2023, § 33 & sched.

share large datasets with several bidders in order to meet the tight timelines of the process. Each bidder who receives raw data becomes another point of risk, even where a confidentiality undertaking has been signed. A confidentiality promise protects the information from public view. It does not ensure that the data is used lawfully or protected against misuse.

C. The Problem of Unequal Voices

The committee of creditors decides the outcome of the process. Employees may have some voice as operational creditors or workmen, but customers, patients and users have none in their capacity as data principals. The fairness concern here is real. The people whose rights are most affected by a data transfer are the least able to influence it.

There is also a danger in the clean slate principle. If a resolution applicant takes over a company together with its data and later claims that earlier privacy defaults are extinguished, individuals may be left without a remedy. The better view is that the clean slate principle protects the applicant from past financial claims, and that the applicant must still follow the DPDP Act for all future processing.

D. Competing Interests

It would be wrong to treat this as a one sided problem. Creditors, including banks and employees owed wages, have a genuine interest in recovering value. A rule that blocks all data transfers could reduce recoveries and make resolution of digital businesses harder. The aim is therefore not to stop transfers but to allow them on lawful and proportionate terms. Data can often be useful to a buyer in anonymised or aggregated form, and a buyer who continues the same business can often honour the original purpose.

V. Comparative Perspectives

A. United States

The United States has dealt with this issue for more than two decades. The leading early example is *FTC v. Toysmart.com, LLC*. Toysmart, an online toy retailer, promised in its privacy policy that customer information would never be shared with third parties. When the company failed, it tried to sell its customer list. The Federal Trade Commission objected, and the matter was settled on conditions that restricted the sale.²³

²³*FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. 2000).

Congress later addressed the problem in the Bankruptcy Code. Where a debtor's privacy policy prohibits the transfer of personally identifiable information, the trustee may sell it only if the sale is consistent with that policy or if a court, after appointment of a consumer privacy ombudsman and a hearing, approves the sale.²⁴ The ombudsman gives the court information on the privacy interests at stake. The model is useful because it puts a voice for consumers into the process without banning sales.

B. European Union

The General Data Protection Regulation requires that personal data be processed lawfully, fairly and for specified purposes, and it allows processing on grounds such as consent, legal obligation and legitimate interests.²⁵ A transfer in insolvency must therefore find a lawful basis and respect purpose limitation. European regulators have generally taken the view that an acquirer of a business takes over the data subject to the same obligations and must inform individuals of the change. The lesson for India is that a sale of a business and a sale of raw data are treated differently. A buyer who continues the business in substantially the same form can more easily justify using the data than a buyer who wants it for an unrelated purpose.

VI. Recommendations

India does not need to copy any foreign model in full. The following reforms would fit the structure of the Code and the DPDP Act.

1. A clear statutory duty. The Code or the regulations under it should state that insolvency professionals must comply with data protection law when handling personal data. This would remove doubt about who is responsible.

2. Clarity in the DPDP framework. The government should clarify, through rules or amendment, whether and when data transfers under a resolution plan or liquidation fall within section 17 or the legitimate use provisions. Leaving the matter open invites inconsistent practice.

²⁴11 U.S.C. §§ 101(41A), 332, 363(b)(1).

²⁵Commission Regulation 2016/679, of the European Parliament and of the Council 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, arts. 5, 6, 2016 O.J. (L 119) 1.

3. Staged and minimal disclosure. Early stage bidders should receive anonymised or aggregated data. Identifiable data should be disclosed only to shortlisted bidders who give binding data protection undertakings, and only to the extent needed to value the business.

4. Purpose compatibility test. A sale of personal data should be allowed only where the buyer will use it for a purpose compatible with the original purpose, or where fresh consent is obtained. This matches the idea of purpose limitation without blocking the sale of the business itself.

5. An independent privacy check. Borrowing from the American ombudsman model, the adjudicating authority could be assisted by an independent expert, or the Data Protection Board could be given a role to advise, in cases where large volumes of sensitive data are involved.

6. Notice to individuals. Where a transfer goes ahead, affected individuals should be told about the change of control and given the chance to exercise their rights, including erasure, in line with the DPDP Act.

7. Secure deletion in failed processes. If a bidder is not selected, it should be required to delete and certify deletion of the data it received.

These steps respect the commercial purpose of the Code. They also reflect the proportionality test from *Puttaswamy*, because they allow data transfers that serve a legitimate aim while limiting the harm to individuals.

VII. Conclusion

The Insolvency and Bankruptcy Code and the Digital Personal Data Protection Act each work well on their own terms. Together, they leave an uncomfortable gap. The Code treats data as an asset to be preserved and sold, and the DPDP Act treats it as a part of the individual's private life. Neither statute tells the resolution professional or liquidator how to reconcile the two.

This gap is likely to matter more as digital businesses enter insolvency in larger numbers. Leaving it unaddressed risks harm to individuals and legal uncertainty for bidders, who may buy a business and discover that its most valuable asset cannot lawfully be used. A clear framework would serve both sides. It would protect the constitutional right to privacy recognised in *Puttaswamy* and it would also give buyers the certainty they need to pay a fair price. Parliament, the Insolvency and Bankruptcy Board of India and the Data Protection Board should work toward such a framework before the first major dispute forces the courts to do so.

Bibliography

Statutes and Regulations

Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1.

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

Digital Personal Data Protection Rules, 2025 (India).

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

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).

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

Insolvency & Bankr. Bd. of India (Insolvency Resolution Process for Corporate Persons) Regulations, 2016 (India).

Insolvency & Bankr. Bd. of India (Liquidation Process) Regulations, 2016 (India).

11 U.S.C. §§ 101(41A), 332, 363(b)(1).

Cases

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

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

Ghanashyam Mishra & Sons Pvt. Ltd. v. Edelweiss Asset Reconstruction Co., (2021) 9 S.C.C. 657 (India).

Innoventive Indus. Ltd. v. ICICI Bank, (2018) 1 S.C.C. 407 (India).

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

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India).

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

Reports

Bankruptcy Law Reforms Comm., Ministry of Fin., Gov't of India, The Report of the Bankruptcy Law Reforms Committee (2015).

Comm. of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).