



Black Boxes in the Field: Trade Secrets, Algorithmic Opacity, and a Tiered Disclosure Framework for AgTech in India

Unmesha S Patil¹, Apurva Bhilare² and
Manu Joseph G³

¹ Vishwakarma University, Pune, India

² Vishwakarma University, Pune, India

³ Vishwakarma University, Pune, India
patilunmesha@gmail.com

Abstract. Agricultural technology platforms in India have now been increasingly contributing to decisions that impact the farmers of the country significantly. This includes routine recommendations on what variety should preferably be planted, the amount of pesticide dosing. It also includes parametric crop insurance triggers under the Pradhan Mantri Fasal Bima Yojana and digital credit scoring channelled through the AgriStack framework. The machine learning models driving these decisions are protected as trade secrets. This generates a structural conflict between commercial confidentiality and accountability. India's trade secrets regime is common-law driven. It is now poised for codification through the Protection of Trade Secrets Bill, 2024. This Act however was designed for static formulae and customer lists. It is therefore structurally ill-equipped to mediate the identified conflict in algorithmic decision-making. This paper uses a doctrinal method anchored in comparative studies to argue that AgTech trade secrets warrant differentiated treatment. This differentiated treatment implies disaggregating the protected asset. It would be divided into training data, model architecture, parameters, and outputs. These would then have customised disclosure obligations proportionate to the harm-potential of the agricultural decision the model informs. The paper draws on the EU Trade Secrets Directive (2016/943) [22], the US Defend Trade Secrets Act (2016), and the EU Artificial Intelligence Act (2024). Through these it extracts four borrowable mechanisms. These are - confidentiality clubs, risk-based classification, explanation rights, and regulator access models. The paper also assesses their feasibility under Indian institutional conditions. The paper proposes a three-tier disclosure framework. It gives an enforcement architecture and supports it by suggestions for concrete amendments to the proposed Trade Secrets Bill and sectoral interventions through the PPV&FR Authority and IRDAI.

Keywords: Trade Secrets · Algorithmic Accountability · AgTech · Plant Variety Protection · Comparative Intellectual Property Law.

1 Introduction

In April 2026, the magazine *Down To Earth* reported the case of Baburao Patil. He is a Maharashtra farmer whose crop loss claim under the Pradhan Mantri Fasal Bima Yojana was rejected. This rejection was based on a satellite-derived yield estimate that classified his loss as ineligible for compensation [11]. This case is not an isolated incident. Under Pradhan Mantri Fasal Bima Yojana's revised operational guidelines, States have been directed to adopt satellite remote sensing for crop area estimation and yield assessment. This Yield Estimation System is based on Technology (YES-Tech). It has reduced reliance on manual Crop Cutting Experiments by approximately 40 per cent in many States by 2026 itself [12]. However, empirical studies of the scheme have documented that farmer mistrust in technology-driven yield estimation, claim ratios averaging 51–69 per cent, and delays in dispensing amounts have led to yield-data quality disputes between insurance companies and States [13].

Farmers like Baburao Patil who want to challenge a payout denial encounter a unique obstacle. Counterintuitively this is in the form an Intellectual Property. The estimating model's logic, the training data on which it was built, and the parameters by which it classified the loss are protected as trade secrets. Under the current legal regime, the insurer is under no statutory obligation to disclose them. Moreover, sectoral regulators have not historically demanded such disclosure. Furthermore, Indian courts have no settled doctrine for compelling production of machine learning systems in litigation. This is not an isolated regulatory gap with no consequence. Decisions having significant consequence for Indian farmers are increasingly mediated by machine learning systems. These systems are operated by named platforms[24] like CropIn, DeHaat, Fasal, Mahindra Krish-e, and ITC e-Choupal among them. The internal logic operators of these platforms are characterised as proprietary [1, 2].

The Digital Agriculture Mission was approved by the Union Cabinet on 2 September 2024 with an outlay of Rs. 2,817 crore. It contemplates digital identities for 11 crore farmers alongwith the Krishi Decision Support System and a pan-India deployment of the AgriStack framework [14]. This Mission, amongst other things, has attracted concerns about privacy [20] and data exploitation. This can be seen acknowledged in ministerial replies in the Rajya Sabha [15]. Trade secret law is the legal instrument that provides this opacity. It does so without the public-disclosure quid pro quo demanded by intellectual property law or the supervisory architecture associated with codified intellectual property rights. The 22nd Law Commission's 289th Report of 2024 acknowledged the inadequacy of the prevailing common-law regime with respect to trademarks and proposed the Protection of Trade Secrets Bill, 2024 [3]. The Bill, however has been drafted with conventional categories of confidential information in mind. It therefore does not engage the unique features of machine learning systems deployed in agriculture.

This paper makes three claims. Firstly, the AgTech trade secret is not a unitary asset in that it has components that warrant varying degrees of disclosure and protection. Secondly, accountability demands in this sector arise from four distinct pressure points. Third, a workable solution lies in a tiered disclosure framework that

assess the necessity of disclosure against the risk associated with non-disclosure. Section 2 sets out the methodology;

2 Methodology

This paper adopts a doctrinal method, supplemented by comparative analysis[19]. The doctrinal core primarily consists of a detailed analysis of legislative documents like the Protection of Trade Secrets Bill, 2024 [3], the Protection of Plant Varieties and Farmers' Rights Act, 2001 [17], the DPDP Act, 2023 [16], and the Bharatiya Sakshya Adhiniyam, 2023. The comparative method is functionalist. That is, it identifies the regulatory function each foreign mechanism performs and asks whether an Indian instrument can achieve the same function under domestic conditions. Four evaluative criteria have been applied to this, viz., Institutional feasibility, doctrinal compatibility, potential of protecting farmer's interest, and administrative cost.

Two jurisdictions are selected for the analysis. The European Union and the United States. These jurisdictions have been chosen on account of having legislated explicitly on the trade-secret and algorithmic-accountability challenge. It is noteworthy that The EU Artificial Intelligence Act of 2024 is the only statutory model anywhere that confronts the conflict directly within a single legislation [9]. What enriches the analysis is also that the two jurisdictions represent contrasting regulatory philosophies. The substantive rights and risk classification in the EU is contrasted with the procedural protective orders and confidentiality clubs in the US. The EU AI Act, additionally, classifies certain agricultural AI deployments as high-risk[10]. The paper is not based on any empirical fieldwork and the comparative scope is limited to two jurisdictions.

3 The Indian Trade Secrets Landscape

3.1 The Common-Law Regime

Trade Secret Protection in India currently flows from three doctrinal sources. The first is contract. Non-disclosure agreements, employment confidentiality clauses, and licensing terms enforceable under the Indian Contract Act, 1872 are the tools to ensure protection of Trade Secrets. These are subject to the restraint-of-trade prohibition in Section 27 of the Act. The second is the equitable action for breach of confidence. This is traceable to *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.* [1948] 65 RPC 203. This has been absorbed into Indian jurisprudence by the Delhi High Court in *John Richard Brady v. Chemical Process Equipments P. Ltd.*, AIR 1987 Del 372. It was reaffirmed in *Mr. Anil Gupta v. Mr. Kunal Dasgupta*, 97 (2002) DLT 257. The third source is a combination of statutory provisions across different legislations. This includes Section 72 of the Information Technology Act, 2000, certain provisions of the Copyright Act, 1957 that deals with instances where confidential information is fixed in expressive form, and also limited criminal provisions [4].

This regime has two consequential deficiencies that are relevant to this paper. Firstly there is no statutory definition of what constitutes a trade secret. Any judicial articulation of the same has also been inconsistent across high courts. Secondly, it

offers no balancing framework for the public-interest, public-health, or safety-related disclosures that algorithmic systems warrant.

3.2 The Protection of Trade Secrets Bill, 2024

The 22nd Law Commission's 289th Report of 2024 has proposed the Protection of Trade Secrets Bill, 2024 [3]. The Bill brings certain novel features to the Indian trade secret regime. Firstly, it adopts the definition of trade secrets given in Article 39 of the Trade Related Aspects of Intellectual Property agreement. This rectifies a significant lacuna in the current system. Secondly it recognizes misappropriation as a distinct cause of action and provides for civil and criminal remedies. Thirdly it incorporates welfare provisions like whistleblower protection, compulsory licensing, and government use during national emergencies. Additionally, it also mandates in-camera proceedings to protect confidentiality during litigation.

The Bill however has one major lacuna in the current context. It does not contemplate the distinctive features of machine learning systems and their impact on the efficacy of the proposed trade mark system. Furthermore, it treats the trade secret as a unitary asset. Therefore it offers no mechanism for graduated disclosure that could balance those public-interest stakes that would fall short of being categorized as national emergency. For agricultural sector, where the stakes are high and can be potentially catastrophic, this is a critical gap.

4 The AgTech Trade Secret: A Disaggregated Taxonomy

Any meaningful analysis of AgTech Trade Secret requires its dissection into four components. Each of these parts calls for a unique protection-and-disclosure profile.

Training data. Machine learning models in agriculture, as anywhere else, are trained on combinations of data sets. These datasets include farmer-supplied data, for example, soil tests and yield reports. They also include platform-collected data like sensor readings and geo-tagged imagery. So also, public datasets like IMD weather, ICAR varietal trial data and proprietary breeding records also form a part of it. Even though these individual components may not necessarily be trade secrets, the aggregation may itself be categorized as a trade secret. Moreover, each data set has its own distinctive legal characteristics. For example, public datasets cannot be the subject of trade secret protection in their original form and farmer-supplied data raises questions under the DPDP Act, 2023 about purpose limitation and the data principal's continuing rights.

Model architecture. This is the formal description of the network. It includes elements like, layers, activation functions, training objectives, hyper-parameters, etc. Architectural choices are a product of substantial engineering investment. They are, in-fact, the foundation of any competitive advantage achieved. For this reason they typically constitute the most defensible trade secret. They also are the component that is least informative to a farmer challenging an adverse decision. Hence they don't create any pressing need for disclosure.

Model weights and parameters. These are the numerical values that result from training of the model. Possession of weights can enable a competitor to effectively reproduce the model. This is the reason disclosure of weights is the disclosure that operators resist the most. However, it is also the disclosure that an external auditor would need, to verify the model's behavior.

Inference outputs and decision logic. This is the layer closest in proximity to the affected farmer. It tells the farmer what the model recommended and explains the reasoning behind it. Counterfactual explanations and feature-importance scores here can be generated without disclosing the weights referred to above [5]. This naturally is a component where accountability demands and protection interests are comparatively more readily reconciled.

A taxonomy matters to this discussion because the present-day debate often proceeds as if accountability requires disclosure of the entire pipeline. It does not. Disclosure requirements of different components may be calculated differently.

5 The Accountability Demands

Accountability pressure on AgTech models arises from four distinct sources. Each of these implicate a different component of the taxonomy.

Regulatory. Sectoral regulators are routinely required to validate inputs, claims, and decision processes. For example, The Protection of Plant Varieties and Farmer Rights Authority must satisfy itself that NDUS testing data underlying registration is reliable. Similarly the Food Safety and Standards Authority of India must assess inputs claimed safe by reference to Machine Learning-derived risk models. On the same lines, The Insurance Regulatory and Development Authority of India, while approving parametric insurance products under the PMFBY architecture, must evaluate the trigger logic by which satellite imagery and weather data are converted into payout decisions [12]. Each demands access to model behaviour beyond outputs alone.

Judicial. Where Machine Learning output is adduced as evidence, either of infringement or of contractual breach or of insurance ineligibility, Section 63 of the Bharatiya Sakshya Adhinyam, 2023 [25] (successor to Section 65B of the Indian Evidence Act, 1872) demands a certificate as to the conditions of generation. The Supreme Court in *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 [23], treated the analogous Section 65B requirement as mandatory. Here, Machine Learning output presents distinctive challenges for this compliance. For example, the 'computer' that produced the output is not a single machine instead it is a stochastic model whose behaviour is dependent on training data, weights, and randomised inference paths.

Individual farmer rights. The DPDP Act, 2023 grants data principals certain limited rights relevant to the current context. Section 11 confers a right to summary information about processing, however it stops short of the right to explanation that is

contemplated by GDPR Article 22. A farmer facing an adverse credit, insurance, or contract decision therefore has no enforceable statutory entitlement to a meaningful explanation of the algorithmic reasoning under the current legal regime.

Public interest. Where Machine Learning systems produce harms that have large scale implications, for example, pesticide-dosing recommendations that drive resistance evolution, variety recommendations that erode in-situ genetic diversity, or AgriStack-mediated decisions that systematically disadvantage classes of farmers [15], the affected interests cannot be given justice through individual disclosure rights alone. They demand institutional mechanisms for public-interest scrutiny [6].

6 **Comparative Frameworks: Borrowable Mechanisms**

The comparative analysis is organised in the context of four mechanisms. These can be seen in the EU and US instruments. Furthermore, on application of the four evaluative criteria identified in Section 2, these are amenable to the Indian context. Each mechanism is described in the context of its source jurisdiction and assessed for Indian feasibility. Table 1 summarizes the assessment.

Table 1. Comparative analysis of borrowable mechanisms by Indian feasibility.

Mechanism	EU/US source	Indian feasibility	Adaptation required
Confidentiality clubs	EU Dir. 2016/943 Art. 9; US DTSA protective orders	High; already imported in <i>Ericsson v. Xiaomi</i> line	Sectoral specification of club composition
Risk-based classification	EU AI Act Annex III high-risk categories	High; PPV&FR Authority and IRDAI classify by risk	Statutory authority for AI-tier obligations
Explanation rights	EU AI Act Art. 86; GDPR Art. 22	Moderate; DPDP s.11 partial hook	Counterfactual standard; sectoral specification
Regulator access	EU AI Act Art. 78 confidentiality framework	High; SEBI/RBI/CCI have analogues	Express authority for IRDAI and PPV&FR Authority

6.1 **Confidentiality Clubs and Restricted Access Circles**

Article 9 of the EU Trade Secrets Directive (2016/943) provides for measures that preserve confidentiality during litigation [7]; US courts deploy protective orders permitting expert disclosure under strict undertakings. This could be seen in *Waymo LLC v. Uber Technologies, Inc.* [8]. Indian feasibility is high: the Delhi High Court has imported the mechanism in *Telefonaktiebolaget LM Ericsson v. Xiaomi Technology* and subsequent SEP litigation [10]. The principal adaptation required here is sectoral specification of the composition of the club for AgTech disputes.

6.2 Risk-Based Classification

Annex III of the EU AI Act (2024) classifies enumerated AI deployments as high-risk [9]. The mechanism is institutionally compatible with Indian practice: the PPV&FR Authority and IRDAI both already conduct risk-based product classification. The doctrinal gap here is denotation of a statutory authority rather than capacity.

6.3 Explanation Rights

Article 86 of the EU AI Act confers a right to explanation, building on GDPR Article 22 [9]. Section 11 of the DPDP Act provides a partial provision. Counterfactual explanations [5] are administratively achievable for AgTech firms because they require only inference-time computation and do not compel disclosure of the core competitive advantage conferring factors of weights or architecture.

6.4 Regulator Access Models

Article 78 of the EU AI Act imposes confidentiality obligations on national authorities that receive information in the discharge of duties [9]. Indian feasibility here is high as well. This is because regulators like SEBI, RBI, and CCI already operate well-established privileged-information frameworks. The adaptation required here again is statutory authorisation for IRDAI and the PPV&FR Authority to receive Machine Learning pipeline access under certain analogous safeguards.

The comparative analysis yields a consolidated lesson: the trade secret–accountability tension is not a zero-sum, win-lose concept. Procedural mechanisms can very well permit substantive vindication of both interests. Furthermore the Indian regulatory landscape already contains similar mechanisms in adjacent sectors.

7 A Tiered Disclosure Framework for Indian AgTech

The framework proposed here is intended for adoption through amendments to the Protection of Trade Secrets Bill, 2024, supplemented by sectoral regulation. Its core structural choice is careful calculation. Disclosure obligations vary with the harm-potential of the agricultural decision the model mediates and informs. The framework specifically targets the components of the Machine Learning pipeline that are most informative to the relevant accountability pressure point. Table 2 summarizes the architecture.

Table 2. Tiered disclosure framework for AgTech machine learning systems.

Tier	Decision Type	Disclosure Required	Recipient
1	Routine advisory (variety, dose, timing)	Public model card: data provenance, performance, limitations	Public
2	Material individual (credit, insurance, contract pricing)	Counterfactual explanation; feature attribution	Affected farmer

Tier	Decision Type	Disclosure Required	Recipient
3	Systemic / public-interest (food safety, environment)	Architecture, weights, representative training data sample	Regulator court-supervised confidentiality club +

Tier 1: Routine advisory decisions. Plant Variety recommendations, soil-amendment suggestions, and pest-identification outputs of the kind delivered by CropIn, DeHaat, or ICAR’s mobile advisories shall have a model-card disclosure obligation. The operator must publish a description of the model’s intended use, training-data provenance, performance characteristics across relevant farmer subgroups, and known limitations. No disclosure of architecture, weights, or proprietary training data is required here.

Tier 2: Material individual decisions. Decisions that inform and impact entitlement to credit, insurance payouts under PMFBY, contract pricing, or eligibility for government schemes attract a counterfactual-explanation obligation as discussed in the earlier sections [5]. This means that the operator must, on a request by the affected farmer, provide a counterfactual statement with respect to the smallest change in inputs that would have produced a more favourable outcome for the farmer. This obligation can be satisfied without disclosing weights or architecture.

Tier 3: Systemic and public-interest decisions. Where decisions implicate environmental harm, public health, food safety, or systemic effects on classes of farmers, regulator access to the full pipeline is permitted. This is subject to a confidentiality club analogous to the mechanism deployed by the Delhi High Court in *Telefonaktiebolaget LM Ericsson v. Xiaomi Technology* [10]. The club admits the regulator’s technical experts and, where designated by the court, a court-appointed neutral examiner. It is noteworthy that this type of decisions very well includes decisions made within the Krishi Decision Support System under the Digital Agriculture Mission [14]

7.1 Enforcement Architecture

The framework requires an operating system. There are six essential elements in this context, paired as under:

Classification and self-classification limits. A sectoral lead model is proposed. The PPV&FR Authority classifies variety-related decisions, IRDAI classifies insurance-related decisions, and the Data Protection Board acts as residual classifier for non-sectoral AgTech. Operators submit a self-declared classification at deployment but may self-classify only into Tier 1. Tiers 2 and 3 require regulator concurrence. The sectoral regulator may upgrade, and never downgrade, the tier within 90 days through a reasoned order.

Appeal and review. Operators may appeal against the orders to the relevant Sectoral Appellate Tribunal. Where no relevant Sectoral Tribunal exists, the operators may apply to the National Company Law Appellate Tribunal. At the same time, affected farmers and recognized farmer organizations may petition for a tier upgrade. This is borrowed from the community-rights framework of the PPV&FR Act, 2001 [17]. Mandatory reclassification review will occur every three years or upon material change in deployment. This is similar to the EU AI Act's substantial modification doctrine [9].

Penalties and systemic-harm test. Misclassification penalties are tiered. A genuine error attracts a 30-day cure period. Negligent misclassification triggers penalties under the Bill's misappropriation provisions and entitles farmers to seek tier-appropriate disclosure as a remedy. A wilful misclassification with attributable harm attracts criminal liability under Section 318 BNS, 2023 and additionally a regulatory penalty up to two per cent of Indian turnover. This draws on the DPDP Act structure [16]. Tier 3 is triggered by any one of three indicators, viz.,

- i. Scale, i.e., over 100,000 farmers or above five per cent of any State's gross cropped area;
- ii. public-good externalities, i.e., effects on biodiversity, soil health, water tables, or food safety, documented in regulator complaints or peer-reviewed literature; or
- iii. distributional asymmetry in the form of statistically significant differential outcomes across farmer subgroups by landholding, gender, or social category.

8 Concrete Reform Proposals

The framework calls for four targeted interventions based on mechanisms that Indian law already recognizes.

Amendment to the Protection of Trade Secrets Bill, 2024. A new provision should expressly recognize tiered disclosure obligations for trade secrets that are embedded in automated decision-making systems. And sectoral regulators empowered to specify schedules. Drafting of this section could mirror the structure of Section 100 of the Patents Act, 1970 (use by Government), adapted to the Machine Learning context.

Sectoral regulation under the PPV&FR Authority and IRDAI. The PPV&FR Authority should require Tier 1 model cards [21] for any Machine Learning system whose outputs are submitted in support of variety registration or essential-derivation analysis under the PPV&FR Act, 2001 [17]. IRDAI should mandate Tier 2

counterfactual-explanation rights as a condition of approval for parametric insurance products under PMFBY [12].

Amendment to the Digital Personal Data Protection Act, 2023. Section 11 [16] should be amended to recognize an explanation right for automated decisions of significant effect, with ‘significant effect’ defined by reference to the Tier 2 schedule, drawing on GDPR Article 22.

Procedural rules for evidence. The legislature by amendment to the Bharatiya Sakshya Adhiniyam, 2023, should adopt protocols for the admissibility of Machine Learning-generated output. This would be supplementing the Section 63 regime with model-verification mechanisms that are suited to the identified four-component taxonomy.

9 Conclusion

The conflict between trade secret protection and algorithmic accountability in Indian AgTech is a problem resolvable by deploying the right legal tools. Purposive calculation has the potential to lift trade secret disclosure from a zero-sum game to a system that justly accommodates the interests of all parties involved. This calculation involves disaggregating the asset, mapping the pressure points, and matching disclosure mechanism to the stakes involved. The Protection of Trade Secrets Bill, 2024 offers a rare legislative opportunity to incorporate technology relevant provisions to the trade mark regime in India. The cost of inaction now, will unfortunately be borne disproportionately by farmers least equipped to challenge algorithmic decisions affecting their livelihoods. For a largely agricultural economy like India, may create unanticipated shocks in the days to come.

Acknowledgments. [Acknowledgments to be inserted by authors before final submission.]

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Pasquale, F.: *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press, Cambridge, MA (2015).
2. Burrell, J.: How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society* 3(1), 1–12 (2016).
3. Law Commission of India: Report No. 289 on Trade Secrets and Economic Espionage, with the Protection of Trade Secrets Bill, 2024. Government of India, New Delhi (5 March 2024).
4. Basheer, S.: Trade Secrets Law in India: A Critical Reappraisal. *Journal of Intellectual Property Rights* 17(5), 411–423 (2012).
5. Wachter, S., Mittelstadt, B., Floridi, L.: Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology* 31(2), 841–887 (2018).

6. Katyal, S.K.: Private Accountability in the Age of Artificial Intelligence. *UCLA Law Review* 66, 54–141 (2019).
7. Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets). *OJ L* 157, 15.6.2016.
8. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, codified at 18 U.S.C. §§ 1836–1839.
9. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *OJ L*, 12.7.2024.
10. Basheer, S., Reddy, P.: Trade Secrets and Confidentiality Clubs in Indian Patent Litigation. *Indian Journal of Intellectual Property Law* 12, 1–27 (2021).
11. Down To Earth: When Crop Insurance Fails Farmers: Why India's PMFBY Scheme Needs Urgent Reform (April 2026), <https://www.downtoearth.org.in/agriculture/when-crop-insurance-fails-farmers-pmfby-needs-a-rethink>.
12. Department of Agriculture, Cooperation and Farmers' Welfare: Revised Operational Guidelines, PMFBY. Government of India (2020), <https://pmfby.gov.in>.
13. Kumar, A., Singh, R.K.: Effectiveness of Crop Insurance: An Evaluation of PMFBY in Haryana. *Adv. Consumer Res.* (October 2025).
14. Press Information Bureau: Cabinet approves the Digital Agriculture Mission (Rs. 2817 Cr). Government of India (2 September 2024).
15. Ministry of Agriculture and Farmers' Welfare: Reply to Rajya Sabha USQ No. 485 on AgriStack and Data Privacy (29 November 2024).
16. Government of India: Digital Personal Data Protection Act, 2023.
17. Government of India: Protection of Plant Varieties and Farmers' Rights Act, 2001.
18. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 1869 U.N.T.S. 299 (1994).
19. Zweigert, K., Kötz, H.: *Introduction to Comparative Law*. 3rd edn. Clarendon Press, Oxford (1998)
20. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
21. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I.D., Gebru, T.: Model cards for model reporting. In: *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT '19)*, pp. 220–229. ACM, New York (2019).
22. Aplin, T., Radauer, A., Bader, M.A., Searle, N.: The role of EU trade secrets law in the data economy: an empirical analysis. *International Review of Intellectual Property and Competition Law (IIC)* 54, 826–858 (2023).
23. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
24. Carbonell, I.: The ethics of big data in big agriculture. *Internet Policy Review* 5(1), 1–13 (2016). <https://doi.org/10.14763/2016.1.405>
25. Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

