Title of the paper: **Trade secrets vs. data privacy: navigating the overlap with GDPR and other data protection laws**

Name of Author: Mr. Sahaj Agarwal

Name of Institute/Organization: Jindal Global Law School

Official Designation: Law Student

Journal: The International Journal of Legal Review and Research (IJLRAR)

Tradesecrets vs. data privacy: navigating the overlap with GDPR and other data protection laws

Author: Sahaj Agarwal, a Law Student at Jindal Global Law School

Abstract

Contemporary digital economy is based on the unyielding aggregation, processing, and commercialization of information that creates a deep jurisprudential tension between intellectual property rights, namely trade secrets, and basic data privacy systems. Although the law of trade secrets, which is based on the TRIPS Agreement and local equity, encourages innovation by providing business organizations with commercial exclusivity to confidential information, data privacy laws such as the General Data Protection Regulation (GDPR) and India Data privacy Data Protection (DPDP) Act, 2023, give individuals the right to access, manage, and delete their personal data. This research paper is a critical analysis of systemic overlap and the inherent conflicts of these divergent streams of law. It discusses the philosophical conflict between utilitarian property rights and human dignity by examining how these two theoretical foundations are reflected in modern controversies in the law regarding transparency in algorithms. This paper will assess the recent Court of Justice of the European Union (CJEU) jurisprudence, especially the Schufa case, to show how commercial secrecy is now being questioned more than ever where it interferes with the right to know, the right to explanation. Besides, it also examines the duality of proprietary databases, using the Indian common law paradigms in the case of Navigators Logistics and Eastern Book Company v. D.B. Modak to expose the issues of data portability and the Right to be Forgotten. The paper states that trade secrets and data privacy do not exclude each other but must comply with stringent tests of judicial proportionality. Finally, it suggests a unified structure that uses Privacy- Enhancing Technologies (PETs) and regulatory sandboxes, in which the safeguarding of commercial innovation does not overwhelm basic data rights.

1. Introduction

In the moderninformation era, data exists in a legal duality: it is both the most prized proprietary resource to corporate innovation, and a personal continuation of individual autonomy. This polar has triggered a never-before-seen collision between two different legal realms: the data protection regimes and the law of trade secrets. Historically applied to guard

chemical recipes and production processes, trade secret law has been brutally applied to the

digital world to securethecomplexmachinelearning algorithms and large amounts of data that have becomethebackboneofworldtrade. On the other hand, data protection frameworks, led bytheEuropeanUnionGDPR and such laws have been replicated in subsequent nationallaws,suchastheDPDPAct 2023 in India, have created a human rights paradigm, intendedtoremedycorporateinformational asymmetries.

These regimes intersecttoformahighlyunstable legal environment that is full of contradictions. Whenanartificialintelligencecompany uses millions of consumer data points to train a predictivemodel,theresultantalgorithm and the hand-selected training datasets are ferociously held astradesecrets.Nevertheless,the data subjects that make up that dataset still have statutory rights to know how the data is being processed algorithmically, and requireerasure.Thepaperoffers a critical and detailed discussion of the tension between trade secretsandprivacyof data. It examines the conceptual and philosophical underpinnings ofthetworegimes, and then goes on to the particular battlegrounds: algorithmic transparency,automated decision making and portability of proprietary databases. Through an analysisofthe changing jurisprudence in the European Union and the common law systems of India,the present paper hypothesizes that the tension is resolved through a break of the binaryzero-sum approaches to the law, and that a sophisticated technology-mediated balancingmechanism is the answer.

2. Philosophical andConceptualGrounds

To critically analyse the intersection of tradesecrets and data privacy, it is important to first break down the divergent philosophical justifications on which they are based.

2.1 Utilitarian Justification of Trade Secrets

Intellectual property and trade secrets protection is heavily based on utilitarian economics theory[1], where innovation is encouraged by the law, and unless these inventions are legally secured, companies will not invest enough in research and development, lest their competitors steal it. Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) defines information, in turn, as a trade secret, in that it is a secret, and that it has undergone reasonable efforts to remain secret[2]. Trade secrets, unlike patents, are based on the principle of perpetual concealment, which in turn supports cross-border innovation in the

[1] William Fisher, ‘Theories of Intellectual Property’ (1994) Harvard Law Review 1, 4
[2] Agreement on Trade-Related Aspects of Intellectual Property Rights 1994, art 39(2)

European Union[3] by the Trade Secrets Directive (2016/943)[4]. In the absence of a specific statutory framework, Indian courts protect trade secrets by the doctrine of equitable breach of confidence and the Indian Contract Act, 1872, Section 27,[5]. The jurisprudence has been formulated in Zee Telefilms Ltd v Sundial Communications Pvt Ltd[6] which protects the trade secret on the basis of the good faith and commercial morality.

2.2 Privacy as a basic human right

Data privacy is rooted in the concept of preserving human dignity and autonomy in stark contrast with the commercial utility of trade secrets. The GDPR is a paradigm shift, which entails treating privacy not as just an economic right, but a fundamental human right as per the EU Charter of Fundamental Rights[7]. This is also true in India, where privacy was transformed into a fundamental right in life and liberty under Article 21 of the Constitution due to the landmark case of Justice K.S. Puttaswamy (Retd) v Union of India[8]. This rights-based approach implements itself in strong statutory mechanisms. Article 15 of the GDPR provides data subjects with the Right of Access (Article 15), the Right to Erasure or the Right to be Forgotten (Article 17), and the Right to Data Portability (Article 20)[9]. The three rights aim to lift the veil of corporate secrecy, which is fundamentally inconsistent with non-disclosure imperatives of trade secret law.

3. The Algorithmic Black Box and Automated Decision-Making

The greatest conflict and most litigated between trade secrets and data privacy is the situation of algorithmic transparency. Contemporary financial institutions, job sites, and insurers use proprietary algorithms to determine creditworthiness, screen resumes, and set premiums. Such algorithms are the most distinctly contemporary trade secrets: complicated, very valuable, and highly guarded.

[3]Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1
[4] Mark A Lemley, 'The Surprising Resilience of the Patent System' (2016) 95 Texas Law Review 1, 22
[5] Indian Contract Act 1872, s 27
[6] Zee Telefilms Ltd v Sundial Communications Pvt Ltd [2003] (5) BomCR 404, 412
[7] General Data Protection Regulation (EU) 2016/679, Recital 1
[8] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1
[9] General Data Protection Regulation (EU) 2016/679, arts 15, 17, 20

3.1 The Right of Explanation and Intellectual Property

The GDPR under Article 22[10] provides the right not to be decided by an automated system (such as profiling) with legal consequences or otherwise with material impact on the individual, as under Article 15(1)(h) that the controllers must provide meaningful information about the logic involved[11]. Corporations are frequently using the defence of trade secrets as blanket defence to such requests. They claim that revealing the parameters, the particular weightings and the logic of the architecture of the algorithm would be a violation of their intellectual property, a vulnerability to competitive damage, and possible enabling of users to game the system. The stressor is that algorithms, especially deep neural networks, are black boxes by nature; to understand their reasoning, it is often necessary to disclose the proprietary code or even the carefully selected training data itself[12].

3.2 CJEU jurisprudence: The Schufa Decision and Proportionality

This conflict has recently had to be refereed by the CJEU. In the groundbreaking case of OQ v Land Hessen (SCHUFA Holding AG)[13], the Court discussed the activities of the largest credit- scoring agency in Germany, Schufa, who produced predictive credit scores through a proprietary algorithm, which they were not ready to reveal to the data subjects, citing commercial trade secrets. The CJEU overturned the idea that trade secrets are a blanket exception to transparency requirements. The Court has acknowledged that Article 15 of the GDPR may not have any negative impact on the rights and freedoms of other people, such as trade secrets (as referred to in Recital 63), but this provision cannot be used to withhold all information to the data subject[14]. The provision of a complicated, incomprehensible mathematical formula is not legally adequate in compliance with privacy, but the provision of the raw source code, which is proprietary, is not. This is reflective of enforcement by national Data Protection Authorities (DPAs). One instance is the fines imposed on the food delivery platform Foodinho (Deliveroo) by the Italian DPA (Garante) due to its lack of transparency in terms of its rider-allocation algorithm (it entirely hid the discriminatory impact of the algorithm)[15]. The invocation of trade secrets by the

[10] ibid, art 22

[11] ibid, art 15(1)(h)

[12] Carys J Craig, Critical Copyright Law and the Politics of Intellectual Property (Edward Elgar Publishing 2018) 142

[13] OQ v Land Hessen (SCHUFA Holding AG) Case C-634/21 [2023] ECLI:EU:C:2023:957

[14] General Data Protection Regulation (EU) 2016/679, Recital 63

[15] Garante per la protezione dei dati personali v Foodinho s.r.l. (2021) Provvedimento n. 234, Italian Data Protection Authority

company was dismissed as it fully concealed the discriminatory consequences of the algorithm. The new legal wisdom holds that commercial secrets should not hush the existence of fundamental rights to privacy; a functionally intelligible explanation should be given by the controllers that holds the main intellectual property intact without making the subject of the data a secret[16].

3.3 The Indian Context: A Statutory Vacuum?

Through a critical analysis of the Indian framework, a worrying statutory loophole is apparent. The DPDP Act, 2023[17], even though codifying the right to information regarding the processing of personal data, conspicuously does not provide a direct equivalent to the GDPR in Article 22, of a right to explanation of purely automated decision-making. In India, therefore, the corporation which uses a proprietary algorithm to deny services can easily hide behind the veil of common law trade secrets. Indian data fiduciaries are not subject to a statutory obligation to disclose the logic used, and thus have a much less demanding burden to demonstrate the results of their algorithm. This creates an opportunity to make India a potentially more favorable jurisdiction to AI developers who are keenly protecting their source code, but it leaves Indian data subjects vulnerable to opaque unregulated algorithmic profiling[18]. The upcoming regulations in the DPDP Act should fill this gap, potentially with reference to the proportionality tests that have been developed by the CJEU, to ensure that trade secrets do not entirely swallow the idea of data accountability

4. Customer Lists, Proprietary Databases, and the Portability Paradox

In addition to the sophisticated machine-learning algorithms, the conflict between these legal frameworks is also on the front burner when it comes to proprietary databases. Having a detailed database on customer buying behaviours, geolocations, and psychometrical portraits are huge investments of both time and money, making it a highly valuable trade secret. At the same time, all entries in that database are personal data.

[16] Julie E Cohen, 'What Kind of Property is Intellectual Property?' (2014) 52 Houston Law Review 691, 712

[17] Digital Personal Data Protection Act 2023

[18] Vishwas Devaiah, 'Theoretical Justifications for Intellectual Property' in Intellectual Property Law (e-PG Pathshala 2014) 12

4.1 Jurisprudence of Customer Lists

The situation in the UK and India is similar where copyright law often becomes confounded with protection of trade secrets due to the protection of customer lists. Employers habitually obtain injunctions to avert former employees using customer databases alleging that they are confidential trade secrets. Indian jurisprudence has however shown a high bar to such protection. The Delhi High Court took a strong jurisprudential position in Navigators Logistics Ltd v Kashif Qureshi[19] when the plaintiff sought an injunction in the form of copyright and trade secret protection over a secret list of customers and business contacts. The Court unanimously dismissed this assertion. The High Court based on Eastern Book Company v DB Modak which struck off the sweat of the brow doctrine in favour of the modicum of creativity doctrine, relied on the ratio of the case that a mundane compilation of customer contacts does not necessarily give rise to IP protection[20]. By critically assessing the secrecy requirement of the database[21] (moved to the category of trade secrets), the Court inadvertently conformed to the field of data privacy, and barred corporations from unfairly stockpiling informational data sets that are not of a truly innovative nature.

4.2 Threat of Data Portability and Erasure

In a situation where a database passes the strict test of trade secret protection such as a highly edited, value-added collection of proprietary analytics, the GDPR and analogous regimes pose an existential risk to its integrity by the Rights to Data Portability and to Erasure[22]. The Right to Data Portability (Article 20 of the GDPR) gives a user the right to obtain their personal data in a structured, commonly read, and machine-readable form and transfer it to a direct competitor[23]. Nonetheless, retrieving raw personal information usually jeopardizes the proprietary relational architecture the very way that the company organized, tagged, and formatted the information, which is the trade secret itself [24].

More disruptive is the Right to be Forgotten. In case a large number of users invoke their Right to Erasure, the predictive worth of a proprietary database may crumble. This is a complicated issue of machine unlearning in the context of AI. When a model is trained using

a dataset that

[19] *Navigators Logistics Ltd v Kashif Qureshi* [2018] 254 DLT 307
[20] *Eastern Book Company v DB Modak* (2008) 1 SCC 1
[21] *Navigators Logistics* (n 19) [34]
[22] Lionel Bently and Brad Sherman, *Intellectual Property Law* (5th edn, OUP 2022) 1120
[23] General Data Protection Regulation (EU) 2016/679, art 20(1)
[24] Aaron Perzanowski and Jason Schultz, 'Digital Exhaustion' (2011) 58 UCLA Law Review 889, 902

contains personal data and the user later revokes their consent andrequests the erasure, the privacy advocates claim that the model itself is contaminatedbecause the weighted parameters of the model are affected by the deleted data[25].Ontheother hand, IP scholars contend that the trained model is an abstracted trade secretquiteseparate to the raw personal data, and compelling it to be destroyed would amount toanexpropriation of intellectual property. This crossroad is a highly unresolved, tense borderoflawofmodern technology[26].

5. Information Security: The Convergency of the Synergy

Although the issues of transparency and portability are visible,itisurgently necessary to legislation and data confidentiality. The joint and uncompromising need of strict information security. In order to effectively be a claimant under TRIPS and national laws regarding trade secret protection, a claimant must prove that he has made reasonable efforts in keeping the information secret. It in turn requires physical access control measures, far-reaching non-disclosure agreements (NDAs) and sophisticated cybersecurity infrastructure to be put in place[27]. In parallel, Article 32 of the GDPR and Section 8 of the Indian DPDP Act require that the data fiduciary adopt reasonable security safeguards to avert personal data breaches[28].

The compliance systems are very synergistic in this operational context. By establishing end-to-end encryption, stringent role-based access control, and data loss prevention (DLP) measures, a corporation can protect its intellectual property portfolio and shield against punitive data protection regulatory penalties at the same time. The inability to protect a database does not only subject corporate entities to huge fines by Data Protection Authorities, but it will also legally eliminate the very trade secret itself; as soon as the data is hacked and leaked, it will not be possible to protect it through reasonable means, and it will automatically lose its IP status[29].

[25] Mark A Lemley, 'How Generative AI turns Copyright Upside Down' (2024) 25 Columbia Science & Technology Law Review 190, 205
[26] Shamnad Basheer and Neil Wilkof, Overlapping Intellectual Property Rights (OUP 2012) 215
[27] TRIPS Agreement (n 2) art 39(2)(c)
[28] Digital Personal Data Protection Act 2023, s 8(4)
[29] William Cornish, David Llewelyn and Tanya Aplin, Intellectual Property: Patents, Copyrights, Trademarks & Allied Rights (10th edn, Sweet & Maxwell 2023) 950

6. Bending a Unified Way Ahead: Proportionality and Technology

The journey through the tricky intersection of trade secrets anddata privacy demands breaking out of legal silos. An aligned way forward should incorporate subtle legal understandings, autonomous regulatory control, and the implementation of sophisticated Privacy-Enhancing Technologies (PETs).

6.1 Arbiters of the Regulatory Process and In Camera Proportionality Testing

The strategy of the CJEU, which employs the courts and the DPA as an independent adjudicator is a possible blueprint of the procedure. In the event of a clash between the right to explanation and trade secrets, the controller is not free to judge its own adherence. On the contrary, the supposedly secure information will be presented to an expert supervisory body. This authority should then test strict proportionality test. The transparency necessary to fulfil the rights of the data subject must be customized to reflect the rationale and importance of the particular data inputs concerning that individual, without necessarily requiring the commercial roadmap to be given up to a rival[30]. In the case of India, to achieve this balance, it is necessary to empower the newly formed Data Protection Board (DPB) under the DPDP Act with the necessary technical expertise. Moreover, this over-dependence on common law in trade secrets poses a lot of uncertainty in India. A specific, holistic statutory framework on trade secrets, similar to the US Uniform Trade Secrets Act (UTSA) or the European Union Directive, would give statutory boundaries that would enable courts and regulators to weigh these rights against data protection requirements with more certainty and precision in legal terms[31].

6.2 The Privacy-Enhancing Technologies (PETs) Role

Finally, the ultimate resolution to the issue of trade secrets and data privacy is dependent on technological innovation. Privacy-Enhancing Technologies enable companies not only to economically benefit by using data but also to ensure compliance with privacy mathematically, which is a win-win solution to both regimes.

1. **Differential Privacy:** Corporations can derive very accurate statistical information and train machine learning models without making a person's personal information reversible, by adding

[30] SCHUFA Holding AG (n 13) [58]
[31] Zakir Thomas, 'Overview of Changes to Indian Copyright Law' (2012) 17 Journal of Intellectual Property Rights 324, 330

noise to the dataset, which is calibrated to ensure privacy of the individual, and meets data protection principles such as data minimization[32].

2. **Federated Learning:** It is a decentralized training approach that enables machine learning models to be trained on multiple peripheral devices with local data samples without the raw data being exchanged or centralized. The proprietary algorithm is trained and trained (to refine the corporate trade secret) but the personal information does not go outside the user device (guaranteeing 100% data privacy and removing the possibility of centralized data breaches)[33].

3. **Zero-Knowledge Proofs (ZKPs):** ZKPs are a new paradigm of transparency in algorithms. In GDPR Article 22, a company might utilize a ZKP to demonstrate to a regulator or a data subject that an algorithm acted upon their data justly and without the use of a forbidden bias,yet offers transparency without the proprietary source code or algorithm weights havingto be made public[34].

7. Conclusion

The nexus between trade secrets and data privacy is one of the most challenging and commercially significant boundaries of modern legal jurisprudence. Due to the growing interdependence of the global economy with the artificial intelligence and processing of large amounts of data, tension between the demand to hoard data as an exclusive source of intellectual property and the need to democratize data under the banner of the most fundamental human rights will multiply exponentially. The case law shows that a broad claim of trade secret protection cannot be a company layer of corporate Armor against algorithmic responsibility and data rights anymore. The developing jurisprudence, especially that of the CJEU, demands that the commercial secrecy should yield to the basic rights of transparency and autonomy. On the other hand, the rights to privacy must not be construed in such a broad way as to use data portability and erasure as weapons of expropriation of legitimate intellectual property which would destroy the incentive regimes of technological innovation.

A zero-sum, binary thought paradigm should be actively denounced by the jurisprudence of the future, both in mature regimes such as the European Union and within the rapidly emerging digital regulatory ecosystem of India. The legal system can design a harmonized reality by

codification of explicit statutory trade secret structures, introduction of strict judicial proportionality scrutinies, and ensuring the use of cryptographic Privacy-Enhancing Technologies by a large number of people. The sanctity of personal data and the vitality of commercial innovation are not just present in this optimized structure but complement each other in the pillars of the digital economy.

[32] Kimberly Bagdis, 'The Whole Is Greater than the Sum of Its Parts: A Holistic Approach to TRIPS' (2021) 36 Temple International & Comparative Law Journal 197, 210

[33] Peter Drahos, A Philosophy of Intellectual Property (Routledge 1996) 25

[34] Peter K Yu, 'Five Decades of Intellectual Property and Global Development' (2016) 8 WIPO Journal 1, 15