DATA AS AN IP ASSET
PART II

INTA Data Protection Committee, Best Practices Subcommittee
Committee Term 2024/25

Chair:
Nicola Benz (MLL Legal, Switzerland)
Vice Chair:
Filipe Cabral (Dannemann, Siemsen, Bigler & Ipanema Moreira, Brazil)
Subcommittee Chairs:
Stephanie O. Sparks (Hoge Fenton, United States)
Nicole Foga (Foga Daley, Jamaica)
INTA Staff Liaisons:
Lori Schulman, Erica Vaccarello

Committee Member contributors:
Otavio Padilha Velasco (Soerensen Garcia, Brazil)
Shem Otanga (Cliffe Dekker Hofmeyr, Kenya)
Thomas Boddien (Nordemann, Germany)
Sandra Iriarte (Palomo Abogados, Guatemala)
Simon Casinader (K&L Gates LLP, UK)
James Tumbridge (Keystone Law, UK)
Scott Pink (O' Melveny, United States)
Ngozi Aderibigbe (Gray and Silicon Legal Advisors, Nigeria)
Nadine Martino (Spruson & Ferguson, Australia)
Laila dos Reis Araujo (George August Universität, Germany)
Cathy Wu (Watson & Band, PR China)
Abhishek Nangi (RNA Technology and IP Attorneys, India)
Ricky Xing (Lexfield Law, PR China)
Purnima Thacker (Mulla & Mulla, India)
Carlos J. Diaz Sobrino (BGBG, Mexico)
William Boyer, (Gowling Wlg, Canada)

Table of Contents

I. Introduction and Background

A) Introduction

In an era dominated by digital innovation and data-driven business models, data has become one of the most significant assets for businesses worldwide, spanning virtually all industries. The volume and variety of commercially utilized data has reached unprecedented levels and is expected to increase even further in the future.

Businesses consider their data, such as customer lists, trade secrets, business-critical databases or other forms of business-relevant information not publicly available, as a commercial asset that has value to the business. Naturally, this has created a high demand for legal mechanisms that protect data from unauthorized access, theft, and misuse, while ensuring its integrity and reliability.

This report aims to assess whether existing intellectual property laws in selected jurisdictions offer meaningful protection for data as an intellectual property ("IP") asset, and at the same time, how these frameworks intersect with other laws, such as personal data protection (privacy) laws that must also be observed. The following selected jurisdictions have been surveyed for this purpose: Australia, Brazil, Canada, China, European Union, India, Kenya, Mexico, Nigeria, the United Kingdom, and the United States.

By collecting information about the landscape across these diverse legal systems, this report highlights the similarities and differences in the treatment of data under various national laws. On this basis, it provides practical guidance on the interplay between available forms of protections for data, including copyright, trade secret law, unfair competition, sui generis database rights, privacy and publicity rights, and contractual provisions. It also aims to provide a comparative foundation to assess whether existing frameworks are sufficient or whether new legislative or regulatory approaches — including harmonized solutions — should be considered and advocated by the International Trademark Association (INTA).

B) Background

Despite its strategic and economic importance, data is not subject to a unified legal framework that defines its ownership, control, or permissible uses. Its legal status remains jurisdictionally fragmented and conceptually unsettled. Most systems do not confer property rights in aggregated data per se; rather, protection arises through a constellation of intersecting legal regimes: copyright, trade secret law, contract law, privacy and data protection frameworks, and—where applicable—sui generis database rights.

While no multilateral treaty specifically provides unified protection for data as an IP asset, there are international instruments that influence the national protection regimes. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), under the World Trade Organization (WTO), requires member states to offer protection for trade secrets through the concept of "undisclosed information" in Article 39 TRIPS. TRIPS incorporates principles from the Paris Convention, including protection against unfair competition under Article 10bis, which has been invoked to address unauthorized data use in certain jurisdictions. WIPO continues to play a leading role for soft law development in this area. Since 2019, its Conversation on IP and Frontier Technologies has engaged stakeholders on topics ranging from data rights and data

base protection to the implications of AI-generated content. Although these discussions remain non-normative, [1] and shaping a common vocabulary for emerging regulatory challenges.

The conclusions reached in this report have taken several years to develop and have gone through a number of iterations. Starting from a focus on personal data and the protections in favor of individual data subjects created through the introduction of privacy laws around the world, the scope has been extended to encompass all types of data (personal and non-personal) and a broad range of applicable legal concepts. The report has been written in a time of fast-moving change in capabilities for using and commercializing data and in the quantity of laws and regulations applying to data in the digital age.

Against this backdrop, this report considers whether harmonization of approaches to protection of data as an IP asset would be desirable and if so, applying which concept.

[1] In a United States Patent and Trademark Office Policy Briefing in November 2021, there was a reference to WIPO's 4th Conversation entitled "Data - Beyond AI in a Fully Interconnected World", which took place from 22-23 September 2021. See: https://www.uspto.gov/sites/default/files/documents/20211116-PPAC-Artificial-intelligence-IP-policy-update.pdf. In an IP forum in China in April 2025, WIPO Assistant Director General Kenichiro Natsume spoke about the WIPO Conversations, noting their focus on AI and raising awareness with Chinese policymakers. See https://english.cnipa.gov.cn/art/2025/4/27/art_3090_199397.html

II. Executive Summary

The legal frameworks governing data as an IP asset are fragmented across jurisdictions. While data is increasingly recognized as a strategic economic resource, no jurisdiction currently treats data as a standalone IP right. Instead, existing protections apply only to specific manifestations of data—such as structured compilations, confidential business information, or personally identifiable data—under a patchwork of legal regimes including copyright, trade secrets, contract law, privacy regulations, and, in some cases, sui generis rights.

All surveyed jurisdictions offer several forms of protection for data, but they show a wide divergence in the legal concepts, scope and criteria for protection and in the enforcement mechanisms available. Combined with the unlimited nature of data, which can be transferred instantaneously and used anywhere, this may lead to uncertainty and inefficiencies for businesses wanting to exercise and enforce data rights. Harmonization would appear to be desirable to remove these inefficiencies.

However, as the national approaches taken to protection of data and related legislation differ widely and the procedural laws for enforcement of rights in data also diverge, it is challenging to develop a recommendation for the most appropriate basis for harmonization across jurisdictions. What may be a known concept in one country will be alien in another, and the consequences of introducing an imported legal concept into an established legal system are difficult to predict.

For global stakeholders, the challenge is not merely uncertainty in enforcement of data rights, but how to achieve strategic alignment of data governance models with rapidly evolving legislation in copyright, secrecy, privacy, and AI regulation, which are also generally not harmonized across jurisdictions.

Finally, the interests of brand owners, the members of (INTA, will not necessarily be aligned on the need to protect data in the same way that they are aligned on the need to protect brand rights – different business models have different priorities when it comes to data use and protection. Respecting these various interests, this report does not settle on a recommendation for harmonization of the law on protection of data.

III. Analysis

A) Jurisdictional Analysis

The results of the jurisdictional survey set out in the Appendix set out how the eleven selected jurisdictions protect rights in data. No jurisdiction surveyed currently recognizes data as a standalone IP right, but all have a mix of legal concepts that govern the use and protection of data and the enforcement of rights in data.

B) Key Concepts Used for the Protection of Data

This section summarizes the main concepts for the protection of data as an asset already in place in the selected jurisdictions analyzed for this report. It briefly explains the benefits and limitations of each of the concepts identified, with illustrative examples from the jurisdictions surveyed. For further detail on individual jurisdictions, reference is made to the analysis in the Appendix.

1. Trade Secrets

Trade secrets are an important source of protection for confidential business information and data that derives value from being kept secret, such as algorithms, customer lists, and operational strategies.

In the United States, the Defend Trade Secrets Act (DTSA) provides robust protections, provided businesses take "reasonable measures" to maintain secrecy and can show the economic value of the data. The European Union's Trade Secrets Directive establishes harmonized protections for trade secrets across all EU Member States, making enforcement more predictable.

However, trade secrets are inherently limited. They do not protect against independently derived or reverse-engineered data, leaving businesses exposed to lawful replication. Once the information enters the public domain—whether by breach, accident, or lawful access—the protection towards third parties evaporates.

Cross-border enforcement also presents challenges, as definitions of "reasonable measures" and evidentiary requirements differ widely. For instance, China's Anti-Unfair Competition Law imposes high burdens of proof, making enforcement particularly difficult for foreign entities.

2. Copyright

Copyright laws protect original compilations and creative arrangements of data but do not extend protection to raw or factual information as such. In most jurisdictions—including Canada, the United Kingdom, and Australia—only databases that exhibit a threshold level of creative input may qualify for copyright protection. This requirement excludes raw, unstructured, or machine-generated datasets, which lack the human authorship or intellectual labor required. The United States has adopted a particularly narrow interpretation, Feist Publications v. Rural Telephone Service Co., 499 U.S. 340 (1991) clarified that the mere effort of compiling data ("sweat of the brow") is insufficient and only databases with original or creative arrangements of data are eligible for copyright protection. This distinction leaves many datasets, particularly those without originality in their arrangement or selection of data, unprotected by copyright.

Emerging technologies expose additional gaps in copyright law. In Thaler v. Perlmutter, 687 F.Supp.3d 140, (D.D.C. 2023), affirmed 130 F.4th 1039, (D.C.Cir. 2025), Rehearing en Banc Denied by 2025 WL 1373093, (D.C.Cir., 2025), the U.S. Copyright Office denied protection to an AI-generated work, emphasizing the human authorship requirement. Similarly, ongoing disputes over AI training datasets—such as OpenAI's use of copyrighted works—highlight unresolved questions about originality, fair use, licensing, and derivative rights. Copyright frameworks remain valuable for protecting creative compilations but fail to address the complexities of raw data, machine-generated content, and datasets aggregated at scale.

3. Sui Generis Rights

Sui generis protections safeguard databases created through substantial investment, regardless of originality. The EU Database Directive (Directive 96/9/EC) is the leading example, giving protection to databases in which a substantial investment has been made and prohibiting unauthorized extraction or reuse of databases that meet this threshold. This framework incentivizes investment in data-intensive industries while allowing tailored exceptions for public interest uses, such as education and research.

However, adoption of sui generis rights is limited outside the EU. For instance, Brazil and India rely on unfair competition laws, which lack the specificity of sui generis protections, while China has no equivalent framework. Enforcement also remains uneven, particularly in a cross-border context, where ambiguities regarding scope and duration hinder their effectiveness.

4. Contracts

Contracts are a flexible tool for addressing gaps left by statutory protections. They allow parties to define licensing terms and usage rights for data, particularly in cross-border transactions and emerging contexts such as in connection with AI-generated datasets. Non-disclosure agreements (NDAs) and licensing agreements are commonly used to govern data-sharing arrangements.

However, contractual protections are restricted by privity – they bind only the parties to the agreement. By nature, they can only provide protections between parties who are identifiable in advance; they do not protect against unlawful use of data by a party with which the data holder has no connection. Also, contracts may contain ambiguities or loopholes, leading to disputes over derivative datasets or ambiguous ownership in collaborative projects. Standardized contractual templates aligned with international frameworks, such as TRIPS, could reduce inconsistencies and enhance enforceability across jurisdictions.

5. Unfair Competition

Unfair competition laws address unauthorized exploitation of data that creates market distortions. For example, Brazil prohibits data misappropriation for unfair gain, while India employs similar principles to address unfair practices. These laws provide valuable recourse for businesses in jurisdictions where IP protections, such as trade secrets or sui generis rights, may be insufficient. However, unfair competition laws are often reactive rather than preventive, requiring evidence of harm, bad faith, or dishonest conduct. Their broad scope also makes them less effective for addressing specific challenges, such as unauthorized data scraping or misuse of aggregated datasets.

6. Publicity and Privacy Rights

Publicity rights protect individuals' names, likenesses, and personal identifiers from unauthorized commercial use. These rights are increasingly relevant in AI-driven industries, where biometric data and synthetic media are used for advertising and other purposes. For instance, in the U.S., White v. Samsung Electronics, 971 F.2d 1395 (9th Cir. 1992) held that the unauthorized use of Vanna White's likeness in an advertisement using a look-a-like violated her publicity rights. However, even within the U.S., publicity rights vary by state, leading to inconsistencies in scope and enforcement.

In contrast, the EU integrates publicity rights into broader privacy frameworks, emphasizing personal control. While these frameworks are important for safeguarding individual rights, privacy laws do not address the commercial or proprietary dimensions of non-personal or anonymized datasets. Nor do they grant proprietary rights in personal data, but instead impose limitations on collection, use and transfer.

C) Possible Approaches to Harmonization

Collectively, the existing legal concepts offer only partial and context-specific protection for data as an asset. Their effectiveness depends on the nature of the dataset, the legal system in question, and the surrounding contractual ecosystem. No single mechanism, or combination of them, fully resolves the structural tension between incentivizing data investment and maintaining openness, interoperability, and fairness. This fragmentation—and the rising strategic importance of data in AI, bioinformatics, and real-time analytics—underscores the need for coordinated global strategies.

Although harmonization may be desirable, we are not aware of any arena in which there is consensus on how to achieve it. The question of which approach to take, whether protection as an intellectual property (IP) right, a sui generis right, or through flexible minimum standards, is contentious. Each proposed approach offers distinct advantages but also suffers from significant limitations.

This section examines the three primary approaches that could be taken to harmonization, analyzing their implications, weaknesses, and the reasons why we conclude that none fully addresses the complexities of protection of data as an IP asset.

1. Property-Based Harmonization

The property-based approach treats data as a proprietary asset, granting exclusive ownership rights akin to those for tangible property. This model is in place in jurisdictions including the United States and China. Property-based rights provide clarity in ownership, making licensing arrangements relatively straightforward and facilitating enforcement. A property-based approach supports companies that reinvest heavily in collecting and structuring data.

However, while this approach excels at incentivizing investment, it fails to accommodate data's unique nature. Unlike tangible assets, data is non-rivalrous—it can be used simultaneously by multiple parties without necessarily depleting its inherent value. Granting exclusive ownership over datasets risks monopolizing resources essential for innovation, particularly in collaborative fields like AI and healthcare, where shared access may drive progress. For instance, genomic research and climate modeling rely on collective efforts and open access to datasets, which would be impeded by proprietary restrictions. Critics of a proprietary protection for data argue that treating data as property creates barriers to equitable access and fosters monopolistic behavior, increasing costs for public-interest initiatives. Further complicating this approach is the issue of co-generated data, such as information collected by IoT devices. Determining ownership when multiple stakeholders contribute to a dataset is highly contentious, adding another layer of complexity. While property-based rights offer robust legal protections, their restrictive nature and incompatibility with collaborative data use mean there is strong resistance to global adoption.

2. Sui Generis Harmonization

Sui generis protections aim to safeguard substantial investments in the creation, curation, and maintenance of databases, regardless of their originality. The European Union's Database Directive (Directive 96/9/EC) exemplifies this approach, granting exclusive rights to prevent un-

authorized extraction and reuse of databases while allowing exceptions for public-interest uses such as research, education, and innovation. This EU sui generis right can be considered similar to ownership in that it gives a sort of exclusivity and can be transferred or licensed. However, the protection that the right gives is limited in time to 15 years from the date the database was created or first made publicly available. This balance between the advantages of a traditional ownership approach but for a limited period of time and with exceptions to the holder's exclusive rights in some situations makes sui generis protections particularly attractive to jurisdictions with rising economies such as Brazil and India, which aim to bolster their fast-developing data ecosystems and could do so by adopting similar frameworks.

While sui generis rights strike a more balanced approach than property-based models, they face significant implementation challenges. Global adoption remains inconsistent, with some jurisdictions, e.g. China, lacking equivalent frameworks entirely. This uneven legal landscape currently creates enforcement difficulties, particularly in cross-border contexts where interpretations of sui generis protections vary or such rights are lacking entirely. These difficulties would remain if sui generis rights were to be harmonized partially, but not across all major jurisdictions. Fitting harmonized sui generis rights into established legal systems with their own legal concepts for protection of data is far from easy. Particularly in more litigious jurisdictions, it can be expected that there would be significant resistance to the creation of new rights that may give rise to further grounds for plaintiff claims, given the uncertainty and associated costs that brings. Furthermore, unresolved questions about the scope of sui generis rights complicate their harmonization. Should sui generis rights extend to raw data, or should they remain limited to curated datasets? Expanding protections to raw data risks creating unnecessary restrictions on innovation and access, while a narrow scope may fail to address emerging challenges in new fields such as AI. Additionally, the enforcement of sui generis rights depends on clear definitions of what constitutes "substantial investment," which can vary widely between

jurisdictions. These ambiguities, combined with the lack of global alignment, limit the utility of sui generis protections as a universal framework.

3. Flexible Approach with Minimum Standards

The flexible minimum standards approach offers an alternative that emphasizes baseline protections while allowing jurisdictions to adapt laws to local contexts. Proponents argue that this model avoids the rigidity of harmonization and respects legal diversity. By establishing minimum safeguards—such as remedies for data misappropriation and requirements to prove substantial investment—flexible standards provide a foundation for addressing data-related disputes without overregulating. This adaptability allows jurisdictions with underdeveloped legal systems to build capacity while ensuring compliance with international norms like TRIPS.

Despite its adaptability, the flexible standards model introduces significant challenges. The lack of harmonization leads to fragmented protections, creating uncertainty for industries operating across borders. For example, multinational companies in AI or cloud computing can face diverging interpretations of what constitutes data misappropriation or of the concept of substantial investment, complicating compliance and enforcement. Furthermore, in the absence of an international coordinating body respected by all participating states, flexible standards rely heavily on individual jurisdictions' ability to implement and enforce them effectively, leaving critical gaps in protections for industries operating in regions with weaker legal frameworks. This inconsistency undermines the predictability and uniformity needed for global data protection frameworks, making flexible standards unable to give any real level of certainty to businesses seeking global protection for their data assets.

IV. Conclusion

Despite significant differences in how jurisdictions approach data protection, certain foundational principles are widely accepted. Most jurisdictions agree on the need for baseline protections to incentivize investment and address data misappropriation. The TRIPS Agreement has been instrumental in establishing minimum international standards for intellectual property enforcement, including remedies for unauthorized use of protected works. Similarly, public interest exceptions, such as those allowing data to be used for research, education, and innovation, enjoy broad support. The European Union, for instance, prioritizes access to datasets for academic and public benefit purposes through tailored exceptions under its Database Directive.

However, fundamental disagreements persist over the scope and structure of protections. One of the key differences lies in the prioritization of proprietary rights versus equitable access. The United States emphasizes proprietary rights, promoting commercial exploitation and private sector innovation, whereas other jurisdictions such as India focus on the importance of equitable sharing of data to support societal progress. These divergent priorities create legal and operational challenges, particularly in industries reliant on cross-border data flows, such as artificial intelligence and cloud computing. The inability to align these foundational elements has prevented the emergence of a globally coherent data protection framework.

Despite the wish for harmonization, no single approach—proprietary rights, sui generis protections, or flexible minimum standards— addresses the complexities of data protection in a globalized economy. No single solution can resolve the diverse priorities of jurisdictions, industries, and stakeholders The challenges posed by these limitations call for continued exploration of hybrid frameworks that integrate the strengths of each jurisdiction's approach and the possibilities of private arrangements in contract.

Appendix: Jurisdiction Specific Survey Responses

The following section offers detailed jurisdiction-by-jurisdiction analysis of how national legal systems approach data protection, ownership, and monetization.

1. United States

In the United States, there is not an overarching or a sui generis law for database protection. Instead, data and databases are protected under a range of federal and state intellectual property laws, along with consumer privacy laws.

At the federal level, databases are primarily protected as trade secrets under the Defend Trade Secrets Act, and as compilations under the Copyright Act. State laws provide protection mainly as trade secrets under the Uniform Trade Secrets Act (or similar trade secret laws in those states that have not adopted the UTSA), as well as through contract law. Moreover, consumer privacy laws, such as the **California Consumer Privacy Act** (CCPA), are playing an increasingly significant role in regulating the use and ownership of personal data.

a) Copyright Law

The U.S. Copyright Act protects original expression, not the underlying ideas or facts embodied in that expression.[3] It recognizes compilations as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated or arranged in such a way that the resulting work as a whole constitutes an original work of authorship"[4] (17 U.S.C. § 101).

In the seminal case *Feist Publications Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991), the Supreme Court rejected the "sweat of the brow" doctrine and held that copyright protection requires a minimal degree of creativity. It ruled that a standard white pages telephone directory organized alphabetically did not meet the originality requirement for copyright protection. However, the Court noted that this threshold "is not particularly stringent" and that "the vast majority of compilations will pass this test."

To establish a copyright infringement claim, the plaintiff must show: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original (Feist, at 361)[7] The second prong of this test typically requires a showing of substantial similarity. However, given the factual nature of most databases, courts typically require a showing of "virtual identity" between the original and alleged copy due to the "thin" scope of protection for factual compilations (*Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1439 (9th Cir. 1994)).[8]

Databases used in artificial intelligence training have been the subject of recent legal scrutiny. Developers of generative AI systems have faced lawsuits alleging that the use of public or scraped data to train models infringes the copyright in source content, particularly when databases include curated or expressive compilations. Courts have yet to determine how far copyright extends to datasets used in machine learning pipelines. Meanwhile, AI-generated outputs are not themselves copyrightable under current U.S. doctrine unless sufficient human authorship is involved, as reaffirmed by *Thaler v. Perlmutter*, No. 1:22-cv-01564 (D.D.C. 2023).

b) Trade Secrets Law

Data and databases can also be protected as trade secrets under both federal and state law. At the federal level, the Defend Trade Secrets Act (DTSA), codified at 18 U.S.C. § 1836 et seq., defines trade secrets broadly to include "compilations" and other forms of information that derive independent economic value from not being generally known, provided the owner has taken reasonable measures to maintain secrecy.

Most states have adopted the Uniform Trade Secrets Act, which mirrors the DTSA in defining protectable interests and recognizing misappropriation as the key infringement standard.[10] North Carolina has not adopted the UTSA but has a similar statute, while New York relies on **common law** to govern trade secret misappropriation.

Unlike copyright, trade secrets do not require an original act of authorship. Instead, trade secret protection requires the owner to take "reasonable measures to keep such information secret." This may include limiting access to those who have a need to view the database and are under a confidentiality agreement. In addition, a trade secret violation does not require evidence of copying of protectable subject matter; it requires a showing of "misappropriation."[11] The owner of the database must also take swift action to prevent misappropriation, or the database may lose its trade secret protection and enter the public domain.

Courts have consistently recognized that databases — particularly those not readily obtainable from public sources — may qualify as trade secrets. For example, customer lists containing detailed, non-public business information have been upheld as trade secrets (*Morlife, Inc. v. Perry*, 56 Cal.App.4th 1514 (1997)). Conversely, courts are reluctant to extend protection to data that is 'readily ascertainable' from public sources, such as business directories. The more difficult information is to obtain, and the more time and resources spent compiling the information, the more likely a court will find that it constitutes a trade secret.[13]

As the commercial value of AI systems depends heavily on proprietary datasets, some businesses treat training data compilations as trade secrets, particularly when the data is licensed, purchased, or aggregated at significant cost. However, enforcing trade secret protection over datasets used in machine learning presents challenges, especially where models are trained on publicly available data or where the outputs do not reveal specific source records. Efforts to maintain secrecy—such as using non-disclosure agreements, limiting employee access, and securing storage—are crucial to retaining trade secret status.

Violations may be pursued civilly under the DTSA or applicable state laws, and in some cases, criminal charges may apply under federal theft of trade secrets statutes.

c) Sui Generis ("Sweat of the Brow") Database Law

The United States does not recognize a sui generis database right akin to the European Union's Database Directive. The U.S. Supreme Court in Feist explicitly rejected "sweat of the brow" as a valid basis for protection absent originality. Legislative proposals for sui generis rights have surfaced periodically but have failed to gain traction, primarily due to concerns over innovation restrictions and access to information.

d) Contract Law

Contract law is one of the most flexible and widely used legal tools for protecting data and databases in the U.S., particularly where statutory IP protections fall short. Contracts can define the ownership, collection, access, use, sharing, transfer, licensing and exercise of other derivative rights (aggregation, modification, downstream distribution, etc.). Contracts defining these

rights in data between two or more parties can provide for protection where little or none is available under copyright, trade secret or other IP laws.[2] There will be some exceptions to what parties can agree to under contract law with respect to personal data depending on applicable state privacy and data protection statutes. Businesses routinely use data sharing agreements, license terms, and non-disclosure agreements (NDAs) to allocate control over data.

Contract law is governed by state common law and statutory regimes, including the Uniform Commercial Code (UCC). Recent amendments to the UCC — notably Article 12, adopted in 2022 — address the transfer of property rights in digital assets such as cryptocurrency and tokenized records. While not directly applicable to databases, these developments signal growing recognition of intangible data as commercial property.

All the footnotes:

[2] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (reversing circuit court decision and holding that the contract – i.e., a shrink wrap license – for database software, which was a collection of telephone directories, is enforceable, notwithstanding that it was not copyrightable, and that copyright law does not preempt contract law)

[1] *See*, e.g., Cal. Civ. Code §§ 1798.100-1798.199.100 (the California Consumer Privacy Act as amended by the California Privacy Rights Act).

[2] Cal. Civ. Code § 1798.100(f) ("Nothing in this section shall require a business to disclose trade secrets…").

[3] 17 U.S.C. § 102(b).

[4] 17 U.S.C. § 101.

[5] 499 U.S. 340 (1991).

[6] E.g., Kregos v. Associated Press, 937 F.2d 700 (2d Cir. 1991)(plaintiff's "pitching form" — a form comprised of nine statistics about a pitcher's performance — copyrightable); Widespread Electrical Sales, LLC, V. Upstate Breaker Wholesale Supply, Inc., 2023 WL 8721435 (N.D. Tex. 2023)(finding copyright protection in original selection and arrangement of the facts in the "product accessories and similar product sections" and product specification tables, but not in parts numbers).

[7] Feist, 499 U.S. at 361.

[8] The "copyright in a factual compilation is thin." Id. at 349. "Virtual identity" is the appropriate standard when a plaintiff's work is entitled to only "thin" protection. Apple Computer, Inc. v. Microsoft Corporation, 35 F.3d 1435, 1439 (9th Cir. 1994).

[9] 18 U.S.C. § 1839(3).

[10] UTSA at §1.

[11] Misappropriation is defined as the "disclosure or use of a trade secret of another without express or implied consent by a person who:
(A) Used improper means to acquire knowledge of the trade secret; or
(B)At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was:
(i) Derived from or through a person who had utilized improper means to acquire it;
(ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
(iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
(C) Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake." See, e.g., Cal. Civ. Code § 3426.1(b).

[12] *See*, e.g., Morlife, Inc. v. Perry, 56 Cal.App.4th 1514 (1997)("a compilation, developed over a period of years, of names, addresses, and contact persons, containing pricing information and knowledge about particular roofs and roofing needs of customers using its services" constituted a trade secret.").

[13] "A customer list may be a trade secret, but not all customer lists are trade secrets under Texas law." Guy Carpenter & Co., Inc. v Provenzale, 334 F.3d 459, 467 (5th Cir. 2003) (citing Hyde Corp. v. Huffines, 314 S.W.2d 763, 766 (Tex. 1958)). "Texas courts consistently consider three factors when determining whether a customer list is a trade secret: (1) what steps, if any, an employer has taken to maintain the confidentiality of a customer list; (2) whether a departing employee acknowledges that the customer list is confidential; and (3) whether the content of the list is readily ascertainable." Id. at 766.

[14] **CCPA § 1798.140(v)(3)**

[15] **CCPA § 1798.100(f)**

[16] *See* CONSOLIDATED TRANSACTION, PROCESSING LLC v. TAPESTRY, INC., 2023 WL 6388101 (E.D. Ill. 2023),

The enforceability of database-related contracts is also supported by doctrines such as factual recital presumptions in California (e.g., Cal. Evidence Code § 622), which bolster agreed terms

on data ownership and control. In *ProCD, Inc. v. Zeidenberg,* 86 F.3d 1447 (7th Cir. 1996), the court upheld shrink-wrap licenses even for databases not independently copyrightable, emphasizing that contract rights can coexist with or extend beyond statutory IP protections.

With the rise of AI, contracts have become central to defining how datasets are used in training and inference workflows. Licenses for data use in AI systems frequently include restrictions on scope, duration, attribution, and the right to derive models or outputs. These provisions are critical, given that copyright and trade secret law may not fully resolve disputes over machine-learning data use.

e) Consumer Privacy & Data Security Laws

Ownership or rights in data and databases are also subject to individual privacy protections under federal and state data privacy laws. These laws allow individuals to access, and in some cases, delete, correct, or control the use, sale, or other disclosure of their personal data. Privacy statutes sometimes require balancing consumer rights with businesses' interests in protecting its trade secrets.

Although there is no comprehensive federal privacy law, several sector-specific laws protect personal data, including the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data, the Gramm-Leach-Bliley Act (GLBA) for financial data, and the Electronic Communications Privacy Act (ECPA) for electronic communications.

At the state level, privacy laws are increasingly shaping data governance. The California Consumer Privacy Act (CCPA grant individuals the right to know how their personal data is collected, used, and sold, and the right to request deletion of their data. Importantly, the CCPA exempts businesses from disclosing trade secrets in response to consumer access requests, creating a delicate balance between transparency and protection.

Most state laws distinguish between personal data and aggregate or de-identified data. The latter is not protected under privacy law and may therefore be commercialized or treated as an intellectual property asset — especially when embedded in analytics, customer segmentation tools, or proprietary models.[14].

Furthermore, all 50 states have enacted data breach notification laws requiring businesses to notify individuals when their personal data has been improperly accessed or disclosed.

f) Other Relevant Legal Bases

Beyond copyright and trade secrets, other bodies of U.S. law shape how databases and data-driven systems may be protected or commercialized. Under patent law, databases as such are generally not eligible for protection. The Supreme Court's decision in *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014), reinforced that abstract ideas implemented using conventional computer technology are not patentable. Patent protection may be available for database-related inventions that meet eligibility criteria under 35 U.S.C. § 101, such as novel database architectures or methods for efficient querying or data processing.

In one example, a method using personal data to generate targeted product offers was deemed an unpatentable abstract idea, illustrating the narrow path for data-driven inventions[16].

However, companies may still obtain patents for technical innovations underlying database management systems, data analytics algorithms, or AI training frameworks if they involve inventive concepts.

2. Canada

In Canada, there is no overarching or sui generis law for database protection. Instead, data and databases are protected through common law trade secret principles, copyright law, and contractual agreements. Moreover, privacy laws such as the *Personal Information Protection and Electronic Documents Act (PIPEDA)* regulate the collection, use, and disclosure of personal information. Provincial jurisdictions play a significant role, particularly in areas such as trade secrets and contract law.

a) Copyright Law

Data collected by companies can be protected as a compilation under the Copyright Act. A compilation is defined as "a work resulting from the selection or arrangement of data."[3] However, this protection applies only to the selection or arrangement of data, not to the underlying data itself.

To qualify for copyright protection, a database must involve sufficient originality in how the data is selected or arranged. The Supreme Court of Canada in *CCH Canadian Ltd v. Law Society of Upper Canada, 2004 SCC 1,* clarified that this originality requires the exercise of "skill and judgment." The Court explained that “skill” involves the use of knowledge, developed aptitude, or practiced ability in creating the work, while “judgment” requires discernment or the evaluation of options. The effort must go beyond trivial or mechanical tasks. For example, simply changing the font of a work would not qualify as sufficient originality to merit copyright protection as an “original” work.[4] Similarly, a compilation must not result from a purely mechanical process; for instance, a database would not qualify as original if its data is entered and appears in the database "almost instantaneously."

To establish that a copyrighted database has been infringed, the rights holder must demonstrate two key elements: (1) that copyright subsists in the database (i.e., the database meets the originality requirement and is not a mere copy of another work), and (2) that a substantial part of the database has been copied.

Canadian copyright law does not currently recognize works generated solely by artificial intelligence as protectable. To qualify, the work must result from human authorship involving sufficient skill and judgment. This position aligns with the requirement in CCH that copyright subsists only where intellectual effort is exercised by a human creator. Consequently, AI-generated outputs are not eligible for copyright protection unless a human contributor exercises control over the final expression.

b) Trade Secrets Law

In Canada, trade secrets are primarily protected under the common law tort of **breach of confidence**. Trade secret law falls under the general constitutional jurisdiction of provinces over "property" unless otherwise carved out, such as in the case of patents. While trade secret laws

[3] *Copyright Act*, RSC 1985, c C-42, s 2.
[4] *CCH Canadian Ltd v Law Society of Upper Canada*, 2004 SCC 13 at para 16.

across provinces are generally consistent, variations exist—such as difference in employment laws, which can influence how trade secrets are handled.

Data that is held in confidence can be protected from inappropriate disclosures if three criteria are met: (1) the data is confidential, (2) the data was communicated in confidence, and (3) the data was misused by the party to whom it was communicated. This type of protection is often applied in cases where a company's confidential customer list is used by an ex-employee to develop a competing business shortly after leaving the company.

Furthermore, although trade secret protection is governed by common law, the Uniform Law Conference of Canada adopted the *Uniform Trade Secrets Act* in 1984. While it has not been enacted in any province, it is frequently used as a reference to summarize Canadian legal principles.

The Canadian federal government does not have jurisdiction over trade secret law, however it is a party to international treaties, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS***).*** Article 39 of TRIPS mandates the protection of undisclosed information if it meets the following criteria: the information is not generally known or readily accessible to individuals within the relevant field, the information derives commercial value from its secrecy, and the owner has taken reasonable steps to maintain its confidentiality.

In 2022, the Criminal Code in Canada was amended to include Section 391, which formally defines the term "trade secret" and creates two new offences related to trade secret theft: (1) it is an offence to knowingly obtain, communicate or make available a trade secret by deceit, falsehood or other fraudulent means; and (2) individuals are also liable if they knowingly obtain, communicate, or make available a trade secret that was obtained through the commission of an offence under subsection (1).[5]

It is important to note here that courts in Canada draw a distinction between "proprietary rights" and "property," and it is unclear whether trade secrets are considered "property" for the purposes of theft provisions in the Criminal Code.

c) Sui Generis ("Sweat of the Brow") Database Law

Canada does not recognize a sui generis database right or "sweat of the brow" protection. Courts have rejected "sweat of the brow" arguments in the absence of sufficient originality under copyright law.

d) Contract Law

A breach of confidence allegation in respect of a trade secret is often accompanied by a breach of contract claim, whether it be a commercial contract or an employment contract. While there is no specific legislation governing data contracts, parties are free to negotiate terms that govern the use, confidentiality, and protection of data. Courts assess the enforceability of such terms, often considering compliance with privacy laws such as PIPEDA.

Like trade secret law, contract law in Canada falls under provincial jurisdiction, and therefore contract laws can vary across provinces. For example, and perhaps most notably, Ontario, Canada's largest province, became the first province to prohibit non-compete provisions in employment contracts in 2021.[6] Such provisions, previously a common tool for trade secret

[5] *Shaver-Kudell Manufacturing Inc v Knight Manufacturing Inc et al*, 2018 ONSC 5206 at paras 87-102.
[6] *Employment Standards Act*, 2000, SO 2000, c 41, s 67.2.

protection, are now prohibited under most circumstances. A "non-compete agreement" is defined as "an agreement, or any part of an agreement, between an employer and an employee that prohibits the employee from engaging in any business, work, occupation, profession, project or other activity that is in competition with the employer's business after the employment relationship between the employee and employer ends".[7]

There are two exceptions to this rule: (1) non-compete agreements are enforceable if they are part of the sale of a business and the seller becomes an employee of the purchaser immediately following the sale, and (2) non-compete agreements may apply to individuals holding executive positions, such as Chief Executive Officer, President, Chief Financial Officer, or other C-suite roles.[8]

Historically, Canadian courts enforced restrictive covenants only in "exceptional circumstances", applying a high standard to assess their reasonableness. With the passage of the new legislation, Ontario now categorically prohibits most non-compete agreements, removing the need for this judicial test in employment contexts.

e) Consumer Privacy and Data Security Laws

IP laws protecting data must be balanced against privacy laws. If companies fail to adhere to these laws, they risk losing the protection of their data or facing liability for privacy breaches. In Canada, *PIPEDA* is the primary federal legislation governing privacy in the private sector. It regulates the collection, use and disclosure of personal information. "Personal information" is broadly defined as any "information about an identifiable individual," whether public or private, with limited exceptions.

PIPEDA applies to federal works, undertakings and businesses, and to private sector organizations that collect, use or disclose personal information during commercial activities in provinces that do not have substantially similar legislation and that transfer personal information across provincial or international borders. PIPEDA's application to personal employee information is limited to organizations that are federal works, undertakings and businesses.

In addition to PIPEDA, several provinces have enacted their own privacy laws. Alberta and British Columbia are governed by the Personal Information Protection Act (PIPA), while Québec has implemented the Québec Privacy Act, supplemented by Bill 3, which governs the use of health and social services data in both public and certain private contexts. While these provincial laws are similar in principle to *PIPEDA*, there are important differences in the details. These laws generally extend to all private sector activities involving personal information, not just commercial activities. They also address the collection, use and disclosure of employees' personal information.

While there is no express prohibition on using personal data to train AI systems, such processing must comply with PIPEDA and equivalent provincial privacy statutes. This includes obtaining meaningful consent, disclosing the purpose of use, and enabling individuals to withdraw consent. The use of de-identified data for AI training is not directly regulated, but if re-identification is possible, the data may still fall within the scope of “personal information” under privacy law.

[7] *Employment Standards Act*, 2000, SO 2000, c 41, s 67.1.
[8] *Employment Standards Act*, 2000, SO 2000, c 41, s 67.2.

Moreover, Canadian courts have recognized privacy torts. The Ontario Court of Appeal established the privacy tort of intrusion upon seclusion in *Jones v. Tsige, 2012 ONCA 32* [9]. This allows individuals to bring an action for damages caused by the invasion of their personal privacy, which may give rise to concerns for companies collecting data that is not anonymized.

f) Other Relevant Legal Bases

Databases themselves are not patentable under Canadian law. However, aspects and ideas related to databases, such as innovative systems or processes that utilize databases, can qualify for patent protection if they meet the criteria for novelty and inventive step.

Canada does not currently have specific legislation governing ownership or use of data for training artificial intelligence systems. As of 2024, no statutory framework explicitly addresses the legal status of training datasets, synthetic data, or AI-generated outputs. Instead, these issues fall under existing copyright, contract, and privacy laws. The absence of AI-specific data legislation in Canada highlights an emerging regulatory gap. Current policy debates, including those under Canada's proposed Artificial Intelligence and Data Act (AIDA), may eventually clarify ownership rights over training data and AI-generated content.

3. Brazil

Brazil has developed a comprehensive framework for data protection and intellectual property, primarily through the General Data Protection Law (Lei Geral de Proteção de Dados – LGPD) and existing intellectual property laws. While Brazil does not explicitly define data as an intellectual property (IP) asset, databases and data can receive protection through copyright law, trade secret law, contractual agreements, and consumer privacy regulations. As courts and legislators address emerging challenges related to artificial intelligence (AI), cross-border data flows, and the digital economy, Brazil's legal landscape continues to evolve.

a) Copyright Law

In Brazil, the protection of databases falls under the **Copyright Law (Lei de Direito Autoral)**, which recognizes compilations as eligible works if they exhibit originality in their selection or arrangement. Article 7 (item XIII) of the Copyright Law defines databases as intellectual creations, provided they result from a human creative process. This protection, however, does not extend to the raw data itself, which remains unprotected unless integrated into a copyrightable work.

To qualify for copyright protection, a database must meet the originality requirement— meaning it reflects the author's intellectual effort and skill in organizing or arranging the data. For instance, a database with a distinctive structure or arrangement may satisfy this criterion. However, mere effort or labor in compiling data (the "sweat of the brow" doctrine) is insufficient to grant copyright protection, as originality remains the cornerstone of Brazilian copyright law.

[9] Jones v Tsige, 2012 ONCA 32.

Copyright owners have exclusive rights to authorize or prohibit reproduction, adaptation, distribution, or other forms of use. Any unauthorized copying or exploitation of the database's structure or creative arrangement constitutes infringement, and rights holders may seek remedies under Brazilian copyright law. Case law confirming protection of databases exists, but remains limited, especially regarding overlaps with personal data or generative AI.

Brazilian law does not currently recognize copyright protection for works generated solely by artificial intelligence. Like many jurisdictions, copyright subsists only in works created by a human author. Where AI outputs involve meaningful human involvement—such as annotating training data, curating model inputs, or guiding generative tools—those elements may be protected under the originality requirement.

b) Trade Secrets Law

Trade secrets are protected under the Industrial Property Law (Lei da Propriedade Industrial – LPI), which defines trade secrets as confidential information that provides economic or competitive value and has been subject to reasonable protective measures. Article 195 (items XI and XII) prohibits unauthorized use, disclosure, or acquisition of trade secrets obtained through dishonest or illicit means, such as breach of contract, bribery, or deception.

To qualify for protection, the following criteria must be met: (1) the information must be confidential and not readily accessible, (2) the information must derive commercial value from its secrecy, (3) reasonable steps must be taken to protect its confidentiality, such as internal policies, NDAs, or technical safeguards.

Brazilian law prohibits the unauthorized use, disclosure, or acquisition of trade secrets through improper means, such as theft, bribery, or breach of confidentiality agreements. Trade secrets are frequently used to protect databases that contain valuable, non-public information, such as customer lists, pricing data, or proprietary research. Violations of trade secret protections may result in civil and criminal penalties, including fines and imprisonment.

In recent years, Brazilian courts have applied trade secret protections to cases involving misappropriation of customer lists and proprietary business data. However, the burden of proving that reasonable measures were taken to protect the confidentiality of the trade secret falls on the data owner. This highlights the importance of implementing robust internal policies and legal agreements to safeguard trade secrets.

c) Sui Generis ("Sweat of the Brow") Database Law

Brazil does not generally recognize a sui generis database right or "sweat of the brow" protection.

d) Contract Law

Contract law plays a central role in protecting data and databases in Brazil. The Brazilian Civil Code allows private parties to define rights related to ownership, access, use, and confidentiality of data through legally binding agreements. Common contractual tools include non-disclosure agreements (NDAs), licensing agreements, and data-sharing arrangements. These

are essential for safeguarding datasets, especially when statutory IP protections are insufficient.

Contractual relationships are governed by general principles under Articles 421 and 422 of the Civil Code, including the duty of good faith and the social function of the contract. These principles are increasingly relevant in the negotiation of AI-related data partnerships and licensing frameworks for model training and deployment.

Furthermore, the LGPD mandates that data processing agreements reflect privacy compliance obligations, including transparency, purpose limitation, and accountability. Contracts involving data transfers must address issues such as lawful basis, data subject rights, liability for breaches, and LGPD-compliant international data transfer mechanisms. When personal data is used in AI training, these agreements become critical for ensuring compliance and risk mitigation.

e) Consumer Privacy and Data Security Laws

Brazil's LGPD, enacted in 2018, is the cornerstone of the country's privacy and data protection framework. Modeled after the EU's GDPR, the LGPD regulates the collection, storage, processing, and sharing of personal data and applies to both public and private sectors. It includes extraterritorial provisions, applying to any processing activity that affects individuals in Brazil.

Personal data is broadly defined to include any information that can identify a person directly or indirectly. Data subjects are granted several rights, including access, rectification, erasure, portability, objection to processing, and withdrawal of consent at any time. Data controllers must obtain explicit consent for data processing, and provide clear notices, secure valid consent where necessary, and implement security measures proportionate to risk. The LGPD also includes mandatory breach notification requirements to both affected individuals and the National Data Protection Authority (ANPD) in the event of incidents.

Importantly, Article 4 of the LGPD exempts businesses from disclosure obligations where doing so would reveal trade secrets. This helps preserve proprietary value while fulfilling transparency obligations.

Of particular relevance to data commercialization and AI:

- The LGPD does not expressly prohibit the use of personal data for training AI systems, but such use must be consistent with the original purpose of collection and based on valid legal grounds (e.g., consent, legitimate interest).
- De-identified or anonymized data may fall outside the LGPD's scope. However, if re-identification is reasonably possible, the data may still be treated as personal.
- Article 20 provides data subjects the right to request human review of automated decisions affecting their interests, which has implications for profiling and AI outputs.

Violations of the LGPD can result in significant penalties, including fines of up to 2% of a company's gross revenue in Brazil, capped at 50 million Brazilian reais per infraction. Companies may also face reputational damage and legal liability for non-compliance.

f) Other Relevant Legal Bases

Databases are not patentable under Brazilian law. Article 10 of the Industrial Property Law excludes abstract ideas, business methods, and purely informational structures from patent eligibility. However, systems, methods, or processes that use or manage data in a novel and

inventive technical way—such as AI model optimization algorithms or database compression techniques—may be eligible for patent protection if they satisfy the criteria of novelty, inventive step, and industrial application.

Employment law also intersects with data governance. Under the Consolidation of Labor Laws (CLT), work products created by employees during the course of employment generally belong to the employer unless otherwise agreed. Employers should include express IP assignment and confidentiality clauses in employment contracts, particularly where staff are involved in data labeling, system design, or database curation for AI applications.

4. Mexico

Mexico has a robust and evolving legal framework for data and database protection, structured through a combination of intellectual property laws, trade secret doctrine, contractual arrangements, and data privacy regulation. While there is no sui generis database law or statutory definition of data as an intellectual property asset, Mexican law recognizes and protects databases through a combination of intellectual property rights, confidentiality obligations, and privacy rules. Notably, Article 108 of the FLCL functions as a quasi-sui generis protection for databases that fail to meet the threshold of originality under copyright law. The legal framework continues to evolve as artificial intelligence, automated data processing, and cross-border transfers reshape the role of databases in the economy.

a) Copyright Law

Databases are eligible for protection under Mexico's Federal Copyright Law (Ley Federal del Derecho de Autor, FLCL), which explicitly recognizes compilations as protected works when they demonstrate originality in their selection or arrangement. Article 107 recognizes databases as compilations eligible for protection if they exhibit originality in the selection or arrangement of their content. Article 110 outlines the rights of database owners, including rights to reproduction, adaptation, distribution, and public communication of the database. Importantly, the underlying data is not protected—only the database's form and organization.

Article 108 addresses non-original databases, providing limited protection against unfair competition. This is not a copyright-based protection but rather a related right ensuring control over investment-heavy but non-original compilations. It is especially relevant where databases lack the originality needed for full copyright yet still merit market-based protection.

In the context of AI development, structured databases—such as annotated corpora used in machine learning—may receive protection if human authorship is demonstrated in the curation or labeling process. However, machine-generated outputs from AI systems are not protected under Mexican copyright law, which requires human creative input for authorship.

b) Trade Secrets Law

In Mexico, trade secrets are governed by the Federal Law for the Protection of Industrial Property (Ley Federal de Protección a la Propiedad Industrial). Article 163 defines a trade secret as any confidential information of industrial or commercial application that provides a competitive or economic advantage to its owner.

To qualify as a trade secret, the information must remain confidential, derive commercial value from its secrecy, and be protected by reasonable measures to ensure its confidentiality.

Trade secrets are protected against unauthorized use, acquisition, or disclosure under the law. Misappropriation is defined as any act contrary to good practices and industry standards, including obtaining trade secrets through improper means or violating confidentiality agreements. Importantly, the law includes exceptions such as independent discovery, reverse engineering, and lawful acquisition from third parties without confidentiality obligations.

Employers often protect trade secrets through confidentiality agreements, non-disclosure agreements (NDAs), and non-compete clauses in employment contracts. While non-compete agreements are enforceable in Mexico, they must be reasonable in scope and duration to be upheld by the courts.

The law includes exceptions such as independent discovery, reverse engineering, and lawful acquisition from third parties without confidentiality obligations.

Violations of trade secret protections may result in administrative, civil, and criminal liability. Criminal penalties include imprisonment ranging from two to six years and significant monetary fines. Additionally, courts and administrative authorities, such as the Mexican Institute of Industrial Property, can order injunctive relief, including the seizure of infringing products and cessation of activities.

c) Sui Generis ("Sweat of the Brow") Database Law

Mexico does not recognize a sui generis database right akin to the EU Database Directive. However, Article 108 of the FLCL serves as a functional analogue. It provides limited protection for non-original databases based on the principle of unfair competition. While these databases may not meet the originality threshold for copyright, Article 108 still grants legal control over unauthorized reproduction or reuse.

This mechanism is particularly valuable in commercial contexts where significant investment has been made in collecting or structuring factual information — such as customer lists, price indices, or technical manuals. In this way, Article 108 operates as a quasi-sui generis remedy, similar in spirit to the EU's prohibition on unfair extraction or reutilization under its Database Directive.

Though underutilized in litigation, Article 108 remains a critical fallback where trade secrets or copyright protection cannot be secured, but market-based unfairness is evident.

d) Contract Law

Contract law is a critical tool for defining and protecting data and database rights in Mexico. Under the Civil Code and Commercial Code, parties are generally free to structure agreements that assign ownership, limit access, define permitted uses, and impose confidentiality obligations and penalties for unauthorized disclosure or misuse of confidential data—provided these terms are lawful and consistent with public policy. As a result, data controllers and processors frequently rely on contractual provisions to govern the secondary use and transfer of data.

Contracts governing data and databases may include NDAs, data-sharing agreements, licensing terms, and employment clauses. Such agreements are particularly important for delineating the permissible use of databases in artificial intelligence development. Contracts may address the scope of data use for model training, retention periods, derivative works, and rights in outputs, especially where copyright or trade secret protection is uncertain.

Contracts involving personal data must also comply with the FLPPDHPP. This includes ensuring that privacy notices are issued, data subjects provide informed consent, and cross-border transfers are subject to appropriate safeguards.

e) Consumer Privacy and Data Security Laws

Mexico's primary data protection legislation, FLPPDHPP, governs the collection, processing, and transfer of personal data by private entities. The law is based on internationally recognized principles, including legality, consent, purpose limitation, proportionality, accountability, and information security.

Article 16 of the Mexican Constitution elevates personal data protection to a constitutional right. The National Institute for Transparency, Access to Information and Personal Data Protection (INAI) serves as the supervisory authority and issues guidance on enforcement, consent requirements, anonymization, and international transfers.

FLPPDHPP grants individuals ARCO rights — Access, Rectification, Cancellation, and Opposition — and obliges controllers to issue privacy notices disclosing the purposes and scope of data processing. Article 36 prohibits international data transfers without express consent unless the recipient ensures equivalent data protection standards.

The law also addresses inferred data and profiling, including automated decision-making. Where AI systems use personal or pseudonymized data to generate behavioral profiles or automated outputs, consent and transparency obligations apply. The processing of anonymized or statistical data may fall outside the law's scope, but if re-identification is feasible, it is treated as personal data.

Violations of privacy laws can result in significant financial penalties, as well as criminal sanctions for serious breaches, such as unauthorized access to sensitive personal data for profit.

f) Other Relevant Legal Bases

Databases are not patentable per se under Mexican law. However, data-driven innovations—such as technical systems for automated data extraction or AI model training infrastructure—may be patentable if they meet the standards of novelty and inventive step under Mexico's industrial property regime.

The Federal Criminal Code provides additional protections, criminalizing activities such as unauthorized access, misuse, or theft of databases. Civil remedies such as damages and injunctive relief are also available.

The lack of specific AI legislation in Mexico leaves questions about the ownership and use of AI-generated data unanswered. However, existing laws, such as the FLPPDHPP and trade secret protections, provide a framework for addressing some of these challenges. Mexico's

National Artificial Intelligence Agenda for 2024-2030 aims to address regulatory gaps and promote ethical and responsible AI development.

5. European Union

The European Union (EU) has developed one of the world's most comprehensive legal frameworks for the protection of data and databases. This framework integrates copyright law, sui generis database rights, trade secrets law, contract law, and robust data protection rules. The Database Directive (Directive 96/9/EC) and the Information Society Directive (Directive 2001/29/EC) provide intellectual property protections, while the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) governs personal data. Trade secrets are harmonized across Member States under Directive (EU) 2016/943.

Recent legislation—including the Data Act (2024), Data Governance Act (2023), and the forthcoming Artificial Intelligence Act (AI Act)—extends regulation to non-personal data sharing, interoperability, and AI training practices. These instruments, combined with extensive Court of Justice of the European Union (CJEU) jurisprudence, form the backbone of the EU's evolving digital and data economy.

a) Copyright Law

Copyright protection for databases in the EU is governed by the Database Directive (Directive 96/9/EC) and the Information Society Directive (Directive 2001/29/EC). Under Article 3 of the Database Directive, copyright applies to databases whose selection or arrangement constitutes the author's own intellectual creation. The protection does not extend to the underlying data unless it is part of an original composition.

In Football Dataco v. Yahoo! (C-604/10) and Infopaq International v. Danske Dagblades Forening (C-5/08), the CJEU clarified that originality requires the exercise of personal creative judgment—not mere investment or effort. Databases generated entirely through automated means, such as algorithmic scraping, do not meet this threshold unless human creative input is demonstrably involved.

The Digital Single Market Directive (Directive 2019/790/EU) further adapts copyright law to data-intensive and AI contexts. Article 3 allows text and data mining (TDM) for scientific research by public institutions without authorization. Article 4 permits commercial TDM unless the rights holder has explicitly opted out.

These provisions are directly relevant to AI model training. In Kneschke v. LAION, a German court applied Article 4 to affirm the permissibility of training large language models using copyrighted materials under the TDM exception, while leaving open the question of whether the public distribution of AI-generated outputs would infringe copyright.

Companies developing AI models must assess the applicability of TDM exceptions and ensure that downstream uses remain within lawful bounds. Licensing strategies are increasingly combined with sui generis database rights and trade secret protections to secure valuable training datasets.

b) Trade Secrets Law

Trade secrets in the EU are primarily governed by Directive (EU) 2016/943, which harmonizes the protection of undisclosed know-how and business information across Member States. This directive aligns with Article 39 of the TRIPS Agreement, ensuring consistency with international intellectual property standards. To qualify as a trade secret, information must not be generally known, have commercial value due to its secrecy, and be subject to reasonable steps to main-

tain confidentiality by its holder. These criteria mirror the common law doctrine of breach of confidence, making EU trade secret law internationally compatible.

CJEU has interpreted these protections broadly, covering both traditional trade secrets (e.g., formulas, manufacturing processes) and modern data assets (e.g., AI models, structured datasets, proprietary analytics). In *Sky Plc and Others v. SkyKick UK Ltd* (C-371/18), the court emphasized that business-sensitive information qualifies for trade secret protection if the company has taken reasonable measures to restrict access and enforce confidentiality.

A major challenge in the EU is balancing trade secret protection with competing rights, such as whistleblower protections, freedom of expression, and employee mobility. Article 5 of Directive 2016/943 exempts disclosures that expose misconduct or illegal activity, safeguard journalistic freedom, or involve employees using general industry knowledge rather than misappropriated secrets. This creates legal tension, particularly in industries where employees possess specialized knowledge critical to a company's competitive advantage.

Unlike copyright or patents, trade secrets lack an international registration system, making enforcement complex, particularly in cross-border disputes. A French company suing a German competitor for misappropriation must navigate national procedural rules, despite the harmonization efforts of Directive 2016/943. Additionally, EU competition and data-sharing laws introduce uncertainty, as regulations such as the Digital Markets Act (DMA) (2022) and Data Act (2024) impose obligations that may conflict with trade secret protections, particularly for AI, fintech, and data-driven industries.

To protect trade secrets effectively, companies must enforce confidentiality agreements, implement cybersecurity measures, and ensure compliance with evolving data governance laws. As AI and data-sharing regulations expand, businesses must integrate trade secret strategies with contractual safeguards and alternative IP protections.

c) Sui Generis ("Sweat of the Brow") Database Law

The European Union is unique in granting a sui generis database right under Directive 96/9/EC (the Database Directive), which protects substantial investments in obtaining, verifying, or presenting data, even if the database lacks the originality required for copyright protection. Unlike copyright, which safeguards the creative selection or arrangement of data, the sui generis right protects databases as commercial assets, ensuring that investment in structuring and organizing data remains economically viable.

In British Horseracing Board v. William Hill (C-203/02) and Fixtures Marketing v. OPAP (C-444/02), the CJEU ruled that sui generis protection applies only when there has been substantial investment in structuring the database itself, not in generating its underlying content.

This legal framework has far-reaching implications for industries relying on structured data, such as financial services, telecoms, and AI training. A sports analytics company compiling match statistics or a fintech firm aggregating real-time market data can invoke sui generis database rights to prevent unauthorized data extraction and reuse. However, enforcement is increasingly challenging, particularly in the era of automated data scraping and AI-driven data aggregation. In CV-Online Latvia v. Melons (C-762/19), the CJEU ruled that scraping job listing databases could infringe sui generis rights if the extraction and re-utilization of data were systematic and substantial, reinforcing that even small repeated extractions can amount to infringement.

Despite its broad scope, the sui generis database right has notable limitations. Article 7(5) of the Database Directive prohibits repeated and systematic use of even small portions of a database when it affects its economic value, but fragmented enforcement across EU Member

States has led to inconsistencies. Some national courts have adopted restrictive interpretations of what constitutes 'substantial investment', while others have taken a broader approach. The rise of AI model training has further complicated legal assessments, as courts struggle to determine whether large-scale dataset extraction for machine learning violates database rights.

With AI, big data, and machine learning increasingly dependent on large-structured datasets, the sui generis right is becoming a critical but legally uncertain tool for protecting data-driven business models. Companies aggregating data from multiple sources must assess whether their compiled datasets qualify for protection, while AI developers must navigate database rights compliance when scraping or training models on structured datasets.

Given the practical enforcement challenges and growing regulatory scrutiny, businesses relying on structured data must adopt a multi-layered protection strategy. Many combine sui generis rights with contractual restrictions, technological barriers (such as API limitations), and trade secret protections to prevent unauthorized data use. As litigation over data scraping and AI model training continues to evolve, the application of sui generis database rights in the digital economy remains a key area of legal uncertainty.

d) Contract Law

The EU does not have a harmonized contract law, but Member States share broad principles of freedom of contract and party autonomy. These principles underpin most data governance agreements, including those for data licensing, non-disclosure, AI training, and service provisioning.

The Digital Content Directive (Directive 2019/770/EU) harmonizes certain consumer-facing digital content contracts, primarily in B2C contexts. While it does not govern B2B data licensing directly, it influences general contractual norms regarding transparency, performance standards, and remedies. Contracts remain the primary mechanism for defining rights over data access and reuse, especially when IP rights are inapplicable or limited. Standard terms include: scope of use (e.g., training, benchmarking, inference); data retention policies and deletion triggers; ownership of derivative works or model outputs, confidentiality and audit clauses.

A growing challenge is the enforceability of clickwrap and browsewrap agreements, particularly for web scraping and AI training datasets. While many website terms prohibit data scraping, their enforceability varies. Recent CJEU case law suggests that contractual restrictions may conflict with sui generis database rights, leaving enforcement uncertain in cross-border disputes.

A key limitation of contract law is that it only binds the parties involved, meaning third parties who misappropriate data are not bound unless additional protections, such as trade secrets, apply. This is particularly relevant in AI model training, where large-scale data scraping occurs without formal contracts.

To mitigate risks, businesses typically combine contractual protections with technological enforcement (e.g., access controls, tokens, API restrictions) and trade secret strategies to control high-value data assets.

e) Consumer Privacy and Data Security Laws

The GDPR sets the EU's benchmark for personal data governance. It applies to any organization processing data of EU residents, regardless of the entity's location. Processing must be lawful, fair, and transparent; based on legitimate purposes; and limited to what is necessary.

Data subjects have rights to access, rectification, erasure, restriction, portability, and objection, as well as protection against automated decision-making.

In Google v. CNIL, the CJEU clarified that the right to erasure applies within the EU, but not globally. GDPR also distinguishes between anonymization and pseudonymization—only the former exempts data from the regulation. AI training on personal data thus requires a clear legal basis and inferred or profiled data must be handled with care, especially where re-identification is possible.

The Data Act complements GDPR by addressing non-personal data access and portability, focusing on industrial datasets and IoT environments. Together, these instruments impose layered compliance obligations on companies leveraging data in AI, analytics, and automated systems.

f) Other Relevant Legal Bases

The Charter of Fundamental Rights of the EU guarantees personal data protection under Article 8 and privacy under Article 7. Article 17 protects property rights but does not define data as a standalone form of property. Consequently, data is regulated through access and control frameworks rather than ownership.

The forthcoming Artificial Intelligence Act imposes obligations based on system risk tiers. High-risk AI systems must comply with documentation, transparency, and data governance standards, including requirements that training data be lawful, representative, and free from bias. These rules shape how companies collect and structure datasets for AI development.

Competition law instruments such as the Digital Markets Act and Digital Services Act impose duties on large platforms to prevent self-preferencing, ensure data interoperability, and disclose algorithmic logic. The European Commission's intervention in Google/Fitbit highlights growing scrutiny over data concentration and competitive harms.

Criminal law adds further constraints. The Cybercrime Directive (2013/40/EU) criminalizes unauthorized access, data theft, and system interference. Member States such as Germany and France have domestic statutes allowing criminal and civil actions for trade secret misappropriation involving data.

Under European Patent Office (EPO) practice, data as such is not patentable. However, data-driven technical processes—such as encryption algorithms, data compression, or AI model optimization techniques—may be patented if they produce a concrete technical effect. In decision G 1/19, the EPO affirmed that AI innovations are patentable when solving a technical problem through a technical means.

6. United Kingdom

The United Kingdom (UK) has a structured legal framework for database and data protection, covering copyright law, sui generis database rights, trade secrets, contract law, and data protection laws. Following Brexit, the UK initially retained many EU-derived legal instruments but has since begun to diverge in areas such as AI governance, text and data mining (TDM), database reciprocity, and digital competition oversight.

The Copyright, Designs and Patents Act 1988 (CDPA) protects databases as literary works, while sui generis database rights remain under the Copyright and Rights in Databases Regulations 1997. However, UK database creators lost automatic protection in the EU post-Brexit. Trade secrets law is governed by the Trade Secrets (Enforcement, etc.) Regulations 2018, aligned with EU Directive 2016/943. The Data Protection Act 2018 (DPA 2018) and UK GDPR regulate personal data use, though the proposed Data Protection and Digital Information (No. 2) Bill signals a shift away from EU GDPR standards.

New regulations, such as the Digital Markets, Competition and Consumers Bill, introduce oversight for dominant tech platforms, reflecting elements of the EU's Digital Markets Act (DMA). Unlike the EU's AI Act, the UK favors a flexible, industry-led approach to AI governance. The UK Supreme Court and regulatory bodies (ICO, CMA) continue to shape data and competition law in the evolving digital economy.

a) Copyright Law

The Copyright, Designs and Patents Act 1988 (CDPA) governs copyright protection in the UK. Under Section 3A, databases qualify as literary works if their structure demonstrates originality in selection or arrangement.

A distinct feature of UK copyright law is its recognition of computer-generated works (CGWs) under Section 9(3) CDPA. The author is deemed to be "the person by whom the arrangements necessary for the creation of the work are undertaken." This provision allows for limited copyright protection of AI-generated datasets where human involvement in the arrangement or oversight can be demonstrated.

UK courts have addressed the originality threshold in *Football Dataco Ltd v. Yahoo! UK Ltd* [2012], which confirmed that independent creative judgment—not mere investment—is required. In *Nova Productions Ltd v. Mazooma* Games Ltd [2006], the court ruled that software-generated content does not confer authorship on the end user. *Bailey v. Graham* [2021] reaffirmed that copyright depends on intellectual effort, not financial investment.

Unlike the EU's broader TDM exception under the Digital Single Market Directive, the UK limits TDM to non-commercial research under Section 29A CDPA. A 2023 government proposal to expand this exception was withdrawn following opposition from rightsholders. As a result, AI developers must secure licences for training datasets.

Ongoing legal disputes are shaping UK copyright law for AI and data use. In *Getty Images v. Stability* AI (2025), Getty alleges unauthorized use of its images for AI training, raising questions about fair dealing exceptions. In *Mumsnet v. OpenAI* (2024-2025), the court will determine whether AI models trained on scraped forum data violate copyright protections. The UK government's AI & Copyright Consultation (2024) suggests potential future reforms, including reintroducing a broader TDM exception, establishing new licensing models for AI developers,

and introducing transparency requirements for training datasets to align with evolving EU AI regulations.

b) Trade Secrets Law

Trade secrets are governed by the Trade Secrets (Enforcement, etc.) Regulations 2018, which implement Directive 2016/943, and supplemented by common law doctrines of breach of con

fidence. The foundational case, Coco v. A.N. Clark (Engineers) Ltd [1969], established that information must be confidential, imparted in confidence, and misused to the detriment of the confider.

UK courts have expanded on these principles in modern trade secret disputes. In Force India v. 1 Malaysia Racing [2012], use of confidential data in a rival team was found to constitute misappropriation. Vestergaard Frandsen v. Bestnet Europe [2013] UKSC 31 held that liability requires knowledge of the breach.

A key post-Brexit challenge in trade secret enforcement is that the UK is no longer bound by CJEU rulings. This means that future trade secret litigation may see UK courts diverge from EU interpretations, particularly in areas such as whistleblower protections and employee mobility. For example, UK labor laws differ significantly from the EU, which could affect how whistleblowers and departing employees use trade-secreted information.

A critical difference from the EU is that UK law allows criminal enforcement of trade secret theft under the Computer Misuse Act 1990. This introduces a higher deterrent against hacking, unauthorized data access, and industrial espionage. In contrast, the EU provides only civil enforcement mechanisms, making the UK's criminal penalties for trade secret violations stricter.

For businesses, contractual safeguards remain essential. Companies must enforce restrictive covenants, employee confidentiality agreements, and cybersecurity measures to prevent data misappropriation. Unlike the EU, where labor mobility laws limit restrictive clauses, UK companies can enforce longer non-compete periods, preventing former employees from using sensitive information in competing businesses.

c) Sui Generis ("Sweat of the Brow") Database Law

The UK continues to recognize sui generis database rights under the Copyright and Rights in Databases Regulations 1997, which implemented Directive 96/9/EC into UK domestic law. Protection is available where substantial investment has been made in obtaining, verifying, or presenting data, but not in data creation itself.

However, Brexit introduced a major shift: UK database creators no longer enjoy automatic protection in the EU, while EU-based databases created after January 1, 2021, do not receive protection in the UK unless explicitly granted contractual rights.

Despite this regulatory divergence, the UK's sui generis framework remains fundamentally aligned with its pre-Brexit EU origins. UK courts have applied restrictive interpretations of this standard, consistent with past CJEU case law. In British Horseracing Board Ltd v. William Hill Organization Ltd (2001), a UK court initially found that a betting database qualified for sui generis protection. However, the later CJEU decision restricted the scope, holding that mere creation of race schedules or results was not enough to justify protection unless substantial effort was directed at structuring the database itself. Similarly, in Football Dataco v. Yahoo! [2012], the court confirmed that database rights apply only where investment is made in structuring the database rather than merely generating data.

However, post-Brexit enforcement of database rights is uncertain. While UK courts may still refer to CJEU rulings for consistency, they are no longer bound by them, meaning future cases

could redefine the scope of protection. This uncertainty poses challenges for businesses relying on structured data. Financial services, AI firms, and tech companies that previously relied

on automatic cross-border database rights must now secure contractual protections when operating in both the UK and EU.

A particularly contentious issue involves automated data scraping and AI model training, where companies extract large datasets to train machine learning systems. Given the UK's growing focus on AI regulation, upcoming legal disputes may clarify whether AI training extraction violates sui generis database rights, especially where data is scraped systematically from protected databases. In the absence of explicit UK case law on AI-generated datasets, businesses seeking protection may need to rely on contractual mechanisms rather than database rights alone.

d) Contract Law

Contract law plays a central role in the UK's data governance landscape. The common law principle of freedom of contract allows parties to define ownership, licensing, confidentiality, and usage rights for databases and datasets. This is particularly important given the absence of a statutory definition of data ownership.

UK courts have enforced express and implied confidentiality clauses, as in Force India v. 1 Malaysia Racing [2012], where an implied duty of confidence extended beyond the literal terms of the agreement. Website terms of service attempting to prohibit scraping have faced variable enforcement, with cases such as Clearview AI Inc v. Information Commissioner (2023) illustrating the tension between contractual restrictions and broader regulatory interests in data use.

The UK government has considered expanding TDM exceptions to facilitate commercial AI development, but no such reforms have yet been enacted. As it stands, commercial TDM requires explicit permission from rightsholders. Consequently, AI developers operating in the UK must structure detailed data licensing agreements to avoid liability.

While contract law is flexible, it binds only the contracting parties. Businesses must therefore combine contract-based protections with technological measures (e.g., access restrictions, API controls) and trade secret enforcement to secure data assets.

e) Consumer Privacy and Data Security Laws

The UK GDPR and Data Protection Act 2018 (DPA 2018) form the foundation of the UK's data protection regime, imposing stringent obligations on businesses for the collection, processing, storage, and transfer of personal data. While the UK GDPR mirrors the EU GDPR, Brexit has granted the UK regulatory flexibility to amend or reinterpret data protection rules.

A key divergence emerged with the Data Protection and Digital Information (No. 2) Bill, which aims to streamline GDPR obligations and reduce compliance burdens while maintaining high data protection standards. Additionally, the UK has established alternative international data transfer mechanisms, such as the UK-US Data Bridge, to replace reliance on EU adequacy decisions.

AI training datasets and data scraping remain grey areas under UK law. Unlike the EU, the UK has not introduced an AI Act imposing specific data protection obligations for AI models. However, ongoing litigation, such as Getty v. Stability AI and Mumsnet v. OpenAI, suggests that the intersection of AI, data protection, and copyright law is increasingly critical.

Recent cases, such as Clearview AI Inc and Information Commissioner's Office (2023), highlight the growing tension between AI data use and privacy protections, particularly regarding the use of biometric data without explicit consent.

f) Other Relevant Legal Bases

UK's approach to data governance remains influenced by retained EU law, but Brexit has introduced key divergences in AI regulation, competition law, and criminal enforcement. The Retained EU Law (Revocation and Reform) Act 2023 signals a shift, allowing UK law to deviate from previous EU interpretations, potentially affecting database and copyright protections.

The Human Rights Act 1998 (HRA) incorporates Article 8 of the European Convention on Human Rights (ECHR), protecting privacy rights. UK courts have addressed this in cases involving government surveillance and data retention. UK law follows common law property principles, meaning data itself is not property, though compilations of data (e.g., databases) may be protected under copyright, contract law, or confidentiality agreements, as reinforced in Fairstar Heavy Transport NV v. Adkins [2013].

The UK's AI regulatory approach differs from the EU AI Act, favoring sector-specific flexibility over strict regulation. The AI White Paper proposes a risk-based model with industry-led governance. The UK government abandoned proposals for broad text and data mining (TDM) exceptions, though ongoing consultations may lead to future reforms. Cases like Getty Images v. Stability AI and Mumsnet v. OpenAI continue to shape UK AI copyright enforcement.

The UK Competition and Markets Authority (CMA) is strengthening digital competition oversight. The Digital Markets, Competition and Consumers Bill, currently in Parliament, introduces Big Tech regulations similar to the EU Digital Markets Act but with greater reliance on self-regulation.

The Computer Misuse Act 1990 remains the UK's primary cybercrime statute, criminalizing unauthorized access, data theft, and hacking. Amendments have expanded protections against AI-driven cyberattacks, while the Online Safety Act introduces penalties for deepfakes and AI-generated fraud.

UK patent law follows the EPO model, but courts have shown openness to AI-assisted inventions. In Thaler v. Comptroller-General of Patents [2021], UK courts ruled that AI systems cannot be inventors, though AI-driven innovations may be patentable if they demonstrate a technical contribution beyond data manipulation.

Key Distinctions Between the UK and EU

Legal Area	European Union (EU)	United Kingdom (UK)
1. AI Regulation	**EU AI Act** – Legally binding risk-based framework with mandatory compliance.	**Voluntary, pro-innovation approach** – Industry-led, flexible guidance.
2. Competition Law	**Digital Markets Act (DMA)** – Hard rules on gatekeepers and platform fairness.	**Case-by-case enforcement** – CMA approach is adaptive and less codified.
3. TDM & AI Training Data	**Broad TDM exception** in Copyright Directive, including opt-out for commercial use.	**No broad TDM exception** – Limited scope, though reform proposals exist.
4. Enforcement Mechanisms	**GDPR fines** set global benchmarks for data protection penalties.	**ICO & CMA** have led high-profile enforcement, but lack EU-level harmonization.

Both jurisdictions share core principles but are increasingly diverging in balancing innovation, competition, and data rights.

7. China

China has rapidly built a multifaceted legal framework for data governance, recognizing data as a strategic asset within its digital economy. Although Chinese law does not currently define data as a standalone intellectual property right, databases and data can be protected through a layered regime that includes copyright, trade secrets, contract law, personal information protection laws, and recent regulatory developments focused on artificial intelligence, data security, and cross-border transfers.

China's approach reflects a blend of civil law principles, administrative oversight, and national policy planning. Key legislation includes the Copyright Law, the Anti-Unfair Competition Law (AUCL), the Civil Code, the Personal Information Protection Law (PIPL), the Data Security Law (DSL), and emerging instruments such as the Data Twenty Articles and draft AI regulations led by the Cyberspace Administration of China (CAC).

a) Copyright Law
Under China's Copyright Law, databases or compilations of data that exhibit selectivity or creative arrangement have the potential to be eligible for copyright protection as collective works. Article 15 of the Copyright Law defines collections of data or materials that reflect originality as eligible for copyright protection. However, this protection extends only to the selection and arrangement of data, not the underlying data itself. Article 3 further defines "works" to include intellectual creations expressed in specific forms such as writings, audiovisual works, engineering designs, and computer software.

In the landmark *Shanghai Hantao Information Consulting Co., Ltd. v. Aibang Juxin Technology Co., Ltd.* case, the court ruled that restaurant reviews collected, selected, and arranged on Dianping.com constituted a collective work under the Copyright Law. In this case, Dianping.com successfully claimed copyright infringement after Aibang Juxin replicated its restaurant reviews. The court ruled that Dianping's database qualified as a collective work due to its creative arrangement of content. Nevertheless, copyright protection does not extend to the data itself, only to its selection and arrangement.

Nevertheless, due to the stringent evidentiary standards required of plaintiffs, legal actions concerning digital asset copyright infringements are not commonly pursued in judicial practice. Plaintiffs must establish originality, ownership and infringement to assert a copyright claim over a database. Furthermore, practical challenges posed by user-generated content, such as obtaining consent from individual contributors, further hinder effective copyright enforcement in the digital realm. This highlights the need for a more streamlined and effective approach to protecting digital assets under copyright law.

b) Trade Secrets Law
Trade secrets in China are governed by the **Anti-Unfair Competition Law (AUCL)**, which defines them as technical or commercial information that is not publicly known, has commercial value, and is subject to measures that ensure its confidentiality as technical or business information the right holder.

The Supreme People's Court Interpretation on Trade Secret Cases further clarifies that data used in technical or business operations can qualify for protection if the confidentiality and value thresholds are met. Examples of protected data include lab statistics, client list, technical

know-how, business plan, computer software and algorithms (also eligible for copyright protection), etc.

In Qucheng Export & Import Co., Ltd. v. Wutian Ci et al., the court held that customer data, including names, contact information, transaction records, preferences, and pricing, constituted trade secrets due to its confidential nature and commercial value. It ruled that the defendants violated the plaintiff's trade secret rights by improperly acquiring and utilizing customer data and pricing information for competitive advantage.

Furthermore, criminal liability may be triggered when trade secrets are obtained through improper means, such as theft, fraud, or other illicit methods. This highlights the intersection of the AUCL with criminal law, ensuring that the unlawful acquisition of trade secrets is deterred through penalties that extend beyond civil remedies.

c) Sui Generis ("Sweat of the Brow") Database Law

China currently does not have a sui generis database right or "sweat of the brow" protection. However, the government is actively pursuing initiatives to create a foundational system for data property rights. In this vein, they have announced the "Data Twenty Articles", officially titled *"Opinions of the Central Committee of the Communist Party of China and the State Council on Building a Fundamental Data System to Better Utilize the Role of Data as an Essential Element."* This policy proposes establishing a registration process to grant rights to data handlers and processors, enhancing protections for legally obtained data

Since 2021, pilot programs in key locations like Shanghai, Zhejiang, and Shenzhen are testing models for data registration, transactional applications, and dispute resolution. These initiatives aim to align legal frameworks with emerging data markets while addressing gaps in enforcement and trade regulation. Local regulations, such as Shanghai's and Shenzhen's data laws, emphasize that only legally obtained data can be traded, reinforcing the importance of lawful data acquisition in commercial practices.

d) Contract Law

Contract law plays a significant role in protecting data rights and facilitating data transactions in China, despite not having a standalone contract law, unlike other jurisdictions. It is embedded within the Civil Code, which provides a flexible framework for data-related agreements. Article 464 defines a contract as an agreement to establish, modify, or terminate a civil legal relationship, while Article 465 affirms that contracts formed in accordance with the law are legally binding and protected.

In addition to its contractual provisions, the Civil Code includes explicit protections for personal data. Article 110 guarantees a natural person's right to privacy, while Article 1034 extends legal protection to personal information. Article 1038 further stipulates that information processors are prohibited from disclosing, tampering with, or providing an individual's personal data

to third parties without their consent. Together, these provisions highlight the interplay between contract law and privacy protections in safeguarding personal data.

Under this framework, parties involved in data-related contracts can define specific terms regarding the use, permissions, confidentiality obligations, liabilities for breach, etc. for specific data, such as data transaction contracts, data licensing agreements, data resource development contracts, and others. However, the Civil Code does not provide a precise definition of

data rights and their scope, relying instead on a general provision for the protection of data assets. This vagueness leaves room for interpretation and can create challenges in enforcing data rights through contractual agreements.

The enforceability of data-related contracts was tested in the *Du Peng v. Beijing Zhizhe Tianxia Technology Co., Ltd.* case, where the court upheld the validity of a user agreement requiring consent for personal data collection as a condition for platform access. The plaintiff, despite refusing to content repeatedly, eventually clicked "agree" to continue using the app. The court ruled that the plaintiff's consent constituted a binding agreement under Contract Law. The *"Zhihu Privacy Policy"* and *"Privacy Protection Guidelines"* were deemed valid supplementary clauses to the user agreement. Since no laws or regulations were violated, the defendant's collection and use of personal information were lawful and enforceable.

e) Consumer Privacy and Data Security Laws

China does not have a single, comprehensive data protection law. Instead, its personal information protection framework is built on a complex network of regulations, with three main pillars: the **Personal Information Protection Law** (PIPL), the **Cybersecurity Law (CSL)**, and **Data Security Law (DSL)**. Together, these laws impose stringent security obligations on brand owners and platforms concerning the collection, storage, use, and transfer of personal data.

The **PIPL**, enacted in 2021, is China's first comprehensive personal information protection law. It defines "personal information" broadly, covering any data linked to an identifiable individual, but excludes anonymized data with its legal status remaining unclear. For instance, cybersecurity laws permit the sharing of anonymized data without requiring explicit consent, creating potential ambiguities for businesses navigating data exchanges. Similarly, the **DSL** broadens the regulatory scope by addressing security concerns related to various categories of data, not just personal information. Collectively, these laws serve as the backbone of China's data privacy regime, guided by principles like legitimacy, proportionality, necessity, and transparency. Notably, personal data is treated as an extension of individual dignity, akin to a moral right.

In *Taobao v. Anhui Meijing* (2018), the court held that online behavioral data (browsing, search history) may not carry independent property value when considered in isolation. However, **data products derived through analysis and processing**, such as recommendation models or consumer profiles, do carry commercial value and may be subject to proprietary interests. This distinction is critical in AI systems, which often rely on transforming raw behavioral data into valuable inference models.

Importantly, the court highlighted that individual online behavioral data, in isolation, holds minimal economic value. Unless explicitly stipulated by law or contract, users do not possess independent property rights over such data. However, this raw data remains under the control of users who generate it, and network operators can only process or utilize it as permitted by agreements with users.

By contrast, network data products—those derived through intellectual processing, in-depth analysis, and systematic integration—hold greater commercial value. These products are distinct from raw user data and allow network operators to exercise control and derive economic benefits. Consequently, network operators can claim proprietary interests in such derivative data products, reinforcing their legal standing in cases of unfair competition or unauthorized use.

At the international level, China is party to the Regional Comprehensive Economic Partnership (RCEP), which commits signatories to adopt legal frameworks for data protection and facilitate cross-border data flows (Articles 12.8 and 12.15). The RCEP require member states to adopt legal frameworks for data protection, reflecting China's alignment with global standards.

f) Other Relevant Legal Bases

China continues to expand its broader legal framework around AI, cybersecurity, and digital innovation. While no comprehensive AI law has been enacted, the Cyberspace Administration of China (CAC) has introduced enforceable administrative measures. The 2023 Interim Measures for Generative Artificial Intelligence Services require that training datasets be lawful and that outputs meet standards of safety, accuracy, and fairness. AI providers must avoid infringing privacy, copyright, or national security rules.

Criminal law also applies. Article 219 of the Criminal Law criminalizes the misappropriation of trade secrets, while Article 285 penalizes unauthorized intrusion into computer systems, including unauthorized data extraction.

Under China's Patent Law, while data as such is not patentable, data-driven innovations (e.g., AI-based recommendation algorithms or encryption systems) may be eligible for protection if they demonstrate novelty, inventive step, and technical contribution.

China's Anti-Monopoly Law authorizes the State Administration for Market Regulation (SAMR) to regulate anti-competitive conduct involving data and algorithms. Enforcement has targeted dominant digital platforms engaged in exclusionary data practices, including gatekeeping and discriminatory access.

Finally, while China's Constitution does not mention personal data, the Civil Code recognizes both a right to privacy (Article 110) and protection of personal information (Article 1034), forming the foundation for broader data rights enforcement.

8. India

India is steadily developing its framework for recognizing and protecting data as an intellectual property asset. This framework is built on constitutional protections, statutory safeguards under copyright and contract law, judicial interpretations, and evolving privacy regulations. While there is no specific sui generis database law or codified trade secrets legislation, Indian courts and legislatures rely on a blend of principles to address the complex interplay between individual rights, corporate interests, and technological advancements.

Recent legislative developments, such as the Digital Personal Data Protection Act, 2023 (DPDP Act), underscore India's increasing focus on data governance.

a) Copyright Law

The Copyright Act, 1957, serves as the backbone of India's legal regime for data protection, defining tables, compilations, computer programs, computer databases as "literary work" under Section 2(o). To qualify for protection, the work must be original in its selection or arrangement. In Eastern Book Company v. D.B. Modak, the Supreme Court rejected the "sweat of the brow" doctrine in favor of the "skill and judgment" test, requiring a minimum degree of creativity to

confer protection. This standard has brought Indian copyright law closer to TRIPS compliance and other common law jurisdictions.

Indian courts have built on this principle in subsequent cases, refining the nuances of originality and its application to compilations and databases. For example, in *Burlington Home Shopping v Rajnish Chibber* (61 (1995) DLT 6), the Delhi High Court recognized that customer lists, developed through significant investment of time, labor, and resources could qualify as copyright-protected literary works, provided they demonstrated originality in arrangement or presentation. Similarly, *Macmillan v. Suresh Chunder Deb* recognized that even minor creativity in the arrangement or selection of data could warrant protection. While the structure of such databases may be protectable, raw data itself is excluded from copyright. This poses challenges for enforcement in contexts such as AI development, where datasets often consist of unstructured factual material gathered through automated means.

b) Trade Secrets Law

India does not have a standalone legislation to protect trade secrets and confidential information. Protection is instead derived from a combination of the Indian Contract Act, 1872, principles of equity, judicial precedents, common law doctrines such as breach of confidence (which in effect amounts to a breach of contractual obligation, and hence governed by principles contained in the Contract Act), and Section 72 of the Information Technology Act 2000. These provisions, while collectively forming a framework, rely heavily on judicial interpretation and contractual remedies. Businesses in India primarily protect trade secrets through mechanisms such as non-disclosure agreements (NDAs) and confidentiality clauses. While these agreements offer flexibility in defining the scope of protection, the absence of codified legislation introduces variability and uncertainty in enforcement.

Trade secrets in India encompass a broad range of sensitive business information. The courts have recognized that cost and pricing data, projected capital investments, inventory marketing strategies, and customer lists can qualify as trade secrets when reasonable measures are taken to maintain their confidentiality. These types of proprietary information, integral to competitive advantage, require robust safeguards to ensure their protection.

Indian courts have consistently recognized the importance of protecting trade secrets. In *Dr. Sudipta Banerjee v. L.S. Davar & Company & Ors.* (MANU/WB/0653/2022), the court emphasized the ethical and contractual obligations of employees, prohibiting the disclosure of confidential information acquired during employment. Additionally, the Court also recognized that while the professional entity might not possess trade secrets per se, individuals employed by the entity would likely have access to privileged information. Likewise, in *M/s Lifecell International Private Limited v. Vinay Katrela* (MANU/TN/4323/2020), the Madras High Court ruled that the restriction applies solely to trade secrets that are developed and pertinent to the company's prospects and cannot be disclosed, reinforcing the principle that such information is integral to competitive advantage.

This protection is increasingly important for companies developing proprietary AI models, training pipelines, or analytical frameworks, where disclosure of datasets or methodologies could undermine competitive advantage.

c) Sui Generis ("Sweat of the Brow") Database Law

India does not have a sui generis database right or "sweat of the brow" protection.

d) Contract Law

The Indian Contract Act, 1872 (“Contract Act”), is generally based on the common law principles, and forms the primary framework for protecting proprietary data through private agreements. It allows parties to a contract to have appropriate clauses in the contract for protection of data like a confidentiality clause. As mentioned above, businesses frequently use NDAs and confidentiality clauses to define ownership, restrict access, and safeguard sensitive information.

Courts in India have consistently upheld such agreements. For example, the Delhi High Court in *Burlington Home Shopping v. Rajnish Chibber* enforced a confidentiality clause to restrain an employee from misusing customer data, and in *Dr. Sudipta Banerjee v. L.S. Davar & Co*., the court emphasized the importance of confidentiality agreements in protecting trade secrets and other sensitive business information.

Contractual terms are particularly important in AI-related contexts, such as data licensing for model training, access to third-party APIs, or the distribution of AI-generated content. However, enforceability depends on precise drafting and the ability to demonstrate breach, especially in digital platforms and cross-border collaborations.

e) Consumer Privacy and Data Security Laws

India's legal framework for personal data protection is undergoing significant transformation with the introduction of the Digital Personal Data Protection Act, 2023 (DPDP Act). The Act builds upon the foundational right to privacy enshrined in Article 21 of the Indian Constitution. This principle was emphasized in the landmark *Supreme Court in Justice K.S. Puttaswamy v. Union of India* case, where the Supreme Court emphasized that privacy is intrinsic to human dignity and autonomy, forming the building block for data protection.

The DPDP Act, promulgated on August 11, 2023, but yet to be notified, represents a comprehensive attempt to regulate the processing of personal data. Once implemented, it will apply extraterritorially to entities offering goods or services in India while processing personal data outside its borders. The Act introduces a consent-based framework, requiring data fiduciaries—entities determining the purpose and means of personal data processing—to obtain informed consent from individuals before processing their data. Exceptions to this requirement exist for certain state uses, including national security, sovereignty, and public order. The Act also mandates data fiduciaries (entities which determine the purpose and means of processing personal data) to maintain the accuracy of data, keep data secure, and delete data once its purpose has been fulfilled. Individuals are granted rights to access, correct, and erase their data, along with grievance redressal mechanism overseen by the Data Protection Board (to be established).

Complementing the DPDP Act is the Consumer Protection Act, 2019 (CPA), which addresses unauthorized disclosure of personal information as an unfair trade practice. Section 2(47)(ix) of the CPA empowers the Central Consumer Protection Authority (CCPA) to regulate such

violations. Under this framework, any disclosure of personal information must comply with existing legal provisions to avoid penalties.

Judicial interventions have also played a significant role in shaping India’s privacy landscape. In *WhatsApp LLC vs. Competition Commission of India and Ors,* the Delhi High Court examined the 2016 privacy policy changes by WhatsApp following its acquisition by Facebook, which effectively forced users into a "take-it-or-leave-it" agreement. The court criticized the imbalance of power between users and the platform, highlighting the need for fairness, transparency, and control over personal data. Similarly, in *Swami Ramdev and Ors. vs. Facebook,*

Inc. and Ors, the Delhi High Court addressed intermediary liability, requiring platforms to globally remove defamatory content and implement geo-blocking for illegal content uploaded outside Indian territory.

f) Other Relevant Legal Bases

India does not yet have a unified AI law, but regulatory scrutiny is growing. In 2024, the Ministry of Electronics and Information Technology (MeitY) issued advisories requiring platforms to seek prior approval before deploying unreliable generative AI models or LLMs. These advisories also mandate that AI-generated content be labeled using unique identifiers, with the aim of improving transparency and preventing the spread of misinformation.
Although non-binding, these measures mark the emergence of an administrative framework for AI accountability.

In the area of criminal law, Section 72 of the Information Technology Act, 2000 penalizes unauthorized disclosure of personal data by intermediaries. The Indian Penal Code contains additional provisions for criminal breach of trust, identity theft, and computer-related offences, supporting enforcement against data misuse and trade secret misappropriation.

India's patent law excludes computer programs per se from patentability but allows for the protection of data-driven inventions if they demonstrate a technical effect. Algorithms and AI tools may qualify for patent protection when embedded in a novel and inventive hardware or software application that meets industrial applicability criteria.

Competition law enforcement is evolving to address the role of data in digital markets. The Competition Commission of India has examined whether certain data practices—such as unilateral changes to privacy terms or exclusionary access to user data—constitute abuse of dominance. The Digital Competition Law Committee is currently assessing the implications of data control, network effects, and opacity in algorithmic decision-making on market competition.

Constitutionally, the right to informational autonomy is now considered integral to human dignity under Article 21, even though there is no explicit right to data. This interpretation increasingly influences how courts assess regulatory and contractual constraints on personal data use.

9. Kenya[10]

Kenya has developed a layered legal framework for data and database protection through statutory, constitutional, contractual, and common law mechanisms. While it does not currently recognize data as a standalone intellectual property category, databases, trade secrets, and personal data benefit from protection under the Copyright Act, 2001, the Data Protection Act, 2019 (DPA), the Law of Contract Act, and equitable principles derived from English common law. Kenya's Constitution, court jurisprudence, and international treaty obligations (e.g., TRIPS) further strengthen its evolving data governance architecture.

a) Copyright Law

The Copyright Act, 2001—enacted to align Kenya with the TRIPS Agreement—recognizes compilations and databases as copyrightable "literary works" where they demonstrate originality in the selection or arrangement of content. Although no formalities are required for the protection of copyright as the same is protected automatically upon fixation, Kenya has a voluntary registration system for copyright works through the national rights registry. Section 38(8) of the Copyright Act prohibits unauthorized use of copyrighted works, including databases, and provides remedies for infringement, including damages and injunctions. This section further extends protection to trade secrets embedded in databases, as long as they remain confidential and commercially valuable. For instance, databases containing commercially sensitive information, such as customer lists or technical blueprints, may benefit from copyright protection if they demonstrate originality in their arrangement or compilation.

Kenyan courts have acknowledged copyright protection for databases in cases such as *Webtribe Ltd t/a Jambopay v. Jambopay Express Ltd (2017) eKLR.* The court noted that the plaintiff's database, which was created through significant investment and effort, qualified for protection under the "sweat of the brow" principle. The court emphasized that the misuse of confidential database information by the defendant constituted a breach of copyright and confidentiality, providing the plaintiff with remedies for unjust enrichment and breach of trust.

b) Trade Secrets Law

Kenya does not have a specific law for the protection of trade secrets. Instead, trade secrets are mostly protected through common law and equity, often enforced via contractual mechanisms. The most practical methods of protecting trade secrets include non-disclosure agreements (NDAs) and confidentiality clauses in employment or business contracts. Breaches of these agreements are interpreted on a case-by-case basis by Kenyan courts.

As mentioned above, Kenya is a signatory party to the TRIPS Agreement, which recognizes the protection of undisclosed information as a trade secret. Article 39 of TRIPS states that trade secrets must be confidential, have commercial value, and be subject to reasonable ef

forts to maintain their secrecy. Such measures may include physical access restrictions, digital encryption, personnel policies, and clearly drafted internal protocols.

[10] All of the Kenya footnotes:

[1] British American Tobacco Ltd v Cabinet Secretary for the Ministry of Health & 5 others (2017) eKLR.
[2] British American Tobacco & others v Secretary of State for Health (2016), High Court of the United Kingdom

This principle was reinforced in *Republic v. Anti-Counterfeit Agency Ex Parte Caroline Mangala t/a Hair Works Saloon (2019) eKLR*, where the court acknowledged trade secrets as a distinct category of intellectual property, recognizing their relevance in combating counterfeit trade. Similarly, in *Safaricom Limited v. Transcend Media Group (2020) eKLR*, the court upheld an NDA stipulating that the ownership of intellectual property remained with the disclosing party and that no disclosure would constitute a transfer of rights.

c) Sui Generis ("Sweat of the Brow") Database Law
Kenya does not have a sui generis database right or "sweat of the brow" protection.

d) Contract Law
Kenya's Law of Contract Act is based on English common law principles and provides a flexible framework for protecting trade secrets and confidential information through contractual agreements. Confidentiality clauses and NDAs are widely used to define the rights and obligations of parties concerning sensitive information. In practice, these agreements are easier to enforce due to their contractual nature, which does not impose regulatory burdens on the parties.

The courts have consistently upheld the enforceability of such agreements. For example, in *Safaricom Limited v. Transcend Media Group (2020) eKLR*, the court noted that an NDA explicitly stipulated that intellectual property rights remained with the disclosing party. Similarly, in *Webtribe Ltd t/a Jambopay v. Jambopay Express Ltd (2017) eKLR*, the court ruled that the defendant's actions—misusing confidential information shared during negotiations—violated the confidentiality agreement and resulted in unjust enrichment. Contracts remain the most practical mechanism for protecting trade secrets in Kenya, especially in the absence of a dedicated legislative framework.

e) Consumer Privacy and Data Security Laws
The Data Protection Act, 2019 (DPA), governs the processing of personal data in Kenya. The DPA defines personal data as any information relating to an identified or identifiable natural person and imposes obligations on data controllers and processors to handle such data responsibly. However, once personal data is anonymized, it is no longer considered personal data thus not within the purview of the DPA.

The DPA grants data subjects rights such as access to their data, rectification, and deletion. Organizations processing personal data must obtain informed consent, maintain data security, and adhere to the principles of transparency and accountability. The accompanying Data Protection Regulations, introduced in 2021, provide detailed guidance on compliance requirements, emphasizing the importance of safeguarding personal data in the digital economy.

In addition to the DPA, the Computer Misuse and Cyber Crimes Act criminalize unauthorized access to data under Section 14, offering protection against cybercrimes targeting personal and sensitive data.

f) Other Relevant Legal Bases
Kenya's Constitution of 2010 provides foundational protections for both privacy and intellectual property. Article 31 guarantees the right to privacy, including protection from unnecessary data collection or disclosure. Article 40 protects property rights, including IP, while Article 24 permits lawful limitations to these rights in the public interest. In British American Tobacco v. Cabinet Secretary for Health (2017) eKLR, the Court of Appeal held that limitations on IP rights—such as mandatory market disclosure rules—could be justified to advance public health goals.

AI and emerging data governance are gaining prominence in Kenya's digital agenda. The National ICT Policy, 2020 prioritizes the development and deployment of AI technologies while calling for ethical data use, algorithmic transparency, and digital rights protections. Although Kenya has not enacted a standalone AI law, the ODPC and Communications Authority of Kenya (CAK) are expected to issue sectoral guidance on automated decision-making, profiling, and synthetic data.

Criminal enforcement of data misuse is addressed under the Computer Misuse and Cybercrimes Act, 2018. Section 14 criminalizes unauthorized access to computer systems and databases, complementing civil enforcement mechanisms under IP, contract, and data protection laws.

Finally, Kenya's Industrial Property Act, 2001, allows patent protection for data-driven technical inventions—such as diagnostic algorithms or automated control systems—provided they meet the criteria of novelty, inventiveness, and industrial applicability. Patent filings may also be made through ARIPO (African Regional Intellectual Property Organization), of which Kenya is a member.

While Kenya's competition law regime has not yet centered on data-related dominance cases, the Competition Authority of Kenya (CAK) is increasingly attuned to platform behavior, cross-border data flows, and digital interoperability issues, especially in alignment with COMESA and Smart Africa regional frameworks.

10. Australia

Australian law does not formally recognize data as a distinct intellectual property asset. However, a robust combination of copyright, contract law, confidentiality principles, and privacy regulation provides overlapping protection for databases, trade secrets, and personal data. Gaps persist in the protection of machine-generated content, unstructured data, and AI training datasets, particularly where no human author or contractual boundary is identifiable. Recent regulatory attention has focused on privacy reform, AI accountability, and strengthening deterrents for serious data misuse.

a) Copyright Law

The Copyright Act 1968 (Cth) governs the protection of literary, dramatic, musical, and artistic works, including databases. Copyright protection in Australia extends to the original expression of ideas or information but does not protect the underlying data itself. This distinction aligns with the classic division in copyright law between non-protectable ideas and protectable expression of those ideas. Databases and data compilations may be protected if they involve the original arrangement or selection of information, provided this arises from independent intellectual effort.

Historically, Australia recognized the "sweat of the brow" doctrine, as in Desktop Marketing Systems Pty Ltd v Telstra Corporation Ltd (2002) 119 FCR 491. However, in IceTV Pty Ltd v Nine Network Australia Pty Ltd (2009) 239 CLR 458, the High Court shifted the test to require

original expression, not merely effort or labor. This was reinforced in Telstra Corporation Ltd v Phone Directories Co Pty Ltd (2010) 194 FCR 142, where the court held that copyright requires a discernible author applying creative judgment—not automation.

Courts have expressed caution regarding databases created primarily through automated processes. In Acohs Pty Ltd v Ucorp Pty Ltd (2010) 86 IPR 492, the court showed reluctance to attribute authorship when human involvement in the compilation process is minimal. This position means that copyright is no longer particularly relevant in Australia for corporate data assets. Not only is the collection of data in raw form (often unstructured or semi structured) likely to lack effort of a literary nature, but the data is also often lacking in any meaning absent some effort from the data analyst, and the "author" is usually a machine or computer programmed to collect information automatically. Data is seldom the province of significant human effort and there will rarely be a particular person who could be said to be an author for copyright purposes.

b) Trade Secrets Law

Australia does not have a standalone statute governing trade secrets. Instead, trade secrets are protected through the equitable doctrine of confidentiality. Protection for confidential information remains one of the more valuable remedies for businesses seeking to prevent unauthorized access to proprietary collections of data. This remedy is particularly where the information is not publicly known, or where the nature of its collation or the insights derived from it remain confidential. In contrast, published facts will lack the necessary quality of confidence unless there is a confidential synergistic effect or confidentiality arising solely from their inclusion in the database. A mere non-selective list of publicly available information is unlikely to qualify as confidential information, even if its collation involves significant time and effort.

The duty of confidence is recognized at common law, with the preconditions for enforcing confidentiality outlined in Smith Kline & French Laboratories (Aust) Ltd v. Secretary, Department of Community Services and Health (1990) 22 FCR 73. This case established three key criteria:

1. The information must have the necessary quality of confidence.
2. The circumstances of its disclosure must create an understanding, either explicit or implicit, that it is to be treated as confidential, or the recipient ought to have realized its confidential nature.
3. The unauthorized use or disclosure of the information must result in detriment to the party confiding it.

The duty of confidence extends to third parties who receive confidential information in breach of an obligation of confidence owed by the disclosing party. Remedies for breaches include injunctions to prevent publication and damages for resulting harm. These principles align with Australia's obligations under the TRIPS Agreement, which requires member states to protect undisclosed information as a form of intellectual property.

c) Sui Generis ("Sweat of the Brow") Database Law

Australia does not recognize a sui generis database right. Instead, databases may be protected under copyright law, confidentiality obligations, or contract law. While the "sweat of the brow" doctrine previously influenced database protection, Australian courts have decisively moved toward a stricter originality standard, as explained above.

d) Contract Law

In the absence of explicit data ownership rights, contract law remains the most effective tool for regulating the use, access, and commercialization of data assets in Australia. Licensing

agreements, NDAs, terms of use, and API agreements allow parties to define the boundaries of data usage, including restrictions on redistribution, re-identification, and training of AI models. Contractual terms can specify the permissible purposes of data access (e.g., training, testing, deployment) and outline ownership of any derivative outputs.

However, contractual protections are inherently limited in scope. They bind only the parties to the agreement and do not automatically extend to third parties who acquire data without authorization. This limitation is particularly relevant in the context of web scraping, where individuals or bots collect data from publicly accessible websites. Although many websites include anti-scraping clauses in their terms of service, the enforceability of such provisions—particularly "browsewrap" terms that are not actively acknowledged by the user—has not yet been definitively addressed by Australian courts.

The regulatory implications of scraping were examined in *Clearview AI Inc and Australian Information Commissioner [2023] AATA 1069*, where the court found that scraping biometric data from the internet for use in facial recognition software violated Australian privacy law. While the ruling was based on privacy rather than contract law, it reflects increasing judicial sensitivity to data extraction practices, particularly where sensitive or identifiable information is involved. Nonetheless, in the absence of statutory prohibitions, contract law remains the primary mechanism by which entities attempt to control the commercial and algorithmic reuse of their data.

e) Consumer Privacy and Data Security Laws

The Privacy Act 1988 (Cth) is the key source of privacy and data protection framework, regulating how certain businesses and federal agencies must use and manage "personal information". The Act introduces the 13 Australian Privacy Principles (APPs), which govern the collection, use, and disclosure of personal information, as well as governance and accountability, integrity and correction of personal information, the rights of individuals to access their personal information, and transborder data flows.

Personal information is broadly defined to include any information about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not or recorded in material form or not. Sensitive information, health information and biometric information are subsets of personal information and are subject to additional privacy protections compared to other types of personal information. Common examples of personal information include name, signature, address, telephone number, email address, date of birth, medical records, bank account details, employment details and commentary or opinion about a person. Breaches of the APPs constitute an "interference with the privacy of an individual" and can result in regulatory action, including significant penalties. The Office of the Australian Information Commissioner (OAIC) is responsible for overseeing compliance with the Privacy Act.

Australian businesses with an annual turnover greater than $AU3 million must comply with the Privacy Act, including individuals (including a sole trader), body corporates, partnerships, unincorporated associations, and trusts. Moreover, smaller businesses may also be subject to its provisions if they fall into the following categories of business:

1. The business is related to another business with an annual turnover of $3 million or above.
2. It provides a health service and holds health information, other than in an employee record (for example, a doctor's clinic).
3. It is in the business of buying and selling personal information.

or

4. It is a contracted service provider under a Commonwealth government contract.

The Privacy Act applies extraterritorially to businesses outside Australia that collect or process personal information linked to Australia.[11]

Recent reforms to the Privacy Act have strengthened its enforcement mechanisms, including penalties for non-compliance. Organizations that commit serious or repeated breaches may face fines of up to AU$50 million, three times the value of any benefit obtained through the breach, or 30% of adjusted turnover during the relevant period. The introduction of a Notifiable Data Breach scheme mandates that affected individuals and the OAIC be informed when a data breach is likely to cause serious harm.

f) Other Relevant Legal Bases

Australia is in the process of addressing data governance challenges that fall outside the traditional IP and privacy domains. One major area of reform involves the legal treatment of de-identified data. Currently, the Privacy Act does not regulate such information. However, the Australian government has acknowledged the increasing risk of re-identification and is proposing reforms that would prohibit unauthorized re-identification and extend privacy protections to certain high-risk de-identified datasets. These proposals also include the creation of a statutory tort for serious invasions of privacy, which would create civil liability for unjustified data misuse even in the absence of a regulatory breach.

Sector-specific privacy statutes operate alongside the Privacy Act. For example, the Spam Act 2003 (Cth) governs electronic marketing communications, while the Privacy and Personal Information Protection Act 1998 (NSW) regulates the handling of personal data by New South Wales state agencies. Similar legislation exists in other states and territories. Industry-specific regulations also exist in telecommunications, financial services, and healthcare.

Australia's legal obligations are shaped by several international frameworks. As a member of the World Trade Organization, Australia is bound by the TRIPS Agreement, which mandates protection of undisclosed information as a form of intellectual property. It also adheres to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and it has committed to privacy and digital governance norms through free trade agreements and digital cooperation pacts with the European Union, United States, and regional partners.

Artificial intelligence regulation is emerging as a policy priority. The Australian government has proposed the development of a National Framework for Safe and Responsible AI, which would establish risk-tiered safeguards for high-impact systems, including requirements for transparency, explainability, and fairness. These proposals aim to address bias in AI decision-making, misuse of personal data, and the re-identification of anonymized data in training datasets. In parallel, public consultations have considered whether AI-generated content should carry identifiable labels or provenance metadata.

[11] See https://www.spruson.com/app/uploads/2023/06/sf_au_data_web.pdf

Finally, issues of patentability continue to arise at the intersection of data protection and intellectual property. Under the Patents Act 1990 (Cth), data itself is not patentable, but data-driven innovations—such as algorithms, analytics platforms, or encryption techniques—may qualify if they produce a technical effect. However, ethical and privacy considerations increasingly influence patent examination, particularly where biometric or personal data is embedded in the invention. The *Clearview AI* case, although decided under privacy law, exemplifies the tension between technological advancement and individual rights in the age of data-centric innovation.

11. Nigeria

In Nigeria, the legal framework governing data as an IP asset offers only partial and indirect protection. While personal data enjoys explicit protection under the Nigeria Data Protection Act (NDPA), 2023, there is no sui generis legislation for the protection of non-personal data or databases as proprietary assets. Instead, existing IP laws such as the Copyright Act, 2022, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, and common law principles relating to confidential information provide piecemeal protection. These fall short of an adequate regime that recognizes data especially non-personal data, given that data serves as a valuable resource in today's digital economy.

a) Copyright Law

Copyright is the most prominent protection accorded to the protection of data and databases as an IP asset in Nigeria. The Copyright Act 2022 serves as Nigeria's extant law on copyright protection. Under the Act, data or databases are not expressly defined or protected nor is there a "compilation copyright" regime, as seen in some other jurisdictions. However, by interpretation, certain database works may qualify for protection as "literary works" under Section 2 of the Act, which covers works eligible for copyright. This means that, to qualify for copyright protection, a data compilation must meet the criteria of a literary work. The interpretation section of the Copyright Act defines literary works to include specifically listed materials such as "encyclopedias, dictionaries, directories, anthologies,) written tables and compilations, including table or compilation of data stored or embodied in a computer or any medium"

Notably, under the Copyright Act, data in and of itself is not eligible for protection. Section 2(5) recognizes compilations but makes it clear that copyright in a compilation (like a database) does not confer rights over the pre-existing material or raw data contained in it. Hence, copyright protects the selection and arrangement of data, not the underlying data itself. Section 3(a) also explicitly states that "mere data," ideas, procedures, processes, and principles are not eligible for copyright.

Deductively, for a database to qualify for copyright protection, it must meet the usual requirements for copyright protection, that is:

i. It must be expressed in a fixed form or must be written down
ii. It must exhibit some creativity or originality in the selection or arrangement of the contents of the work.

b) Trade Secrets Law

Nigeria does not currently have a specific law dedicated to the protection of trade secrets. Although Nigeria is a member of TRIPS, it has not yet fully domesticated Article 39, which mandates protection of undisclosed information or trade secrets. Instead, protection can

largely be credited to common law principles and private organizational efforts. Without a specified legislation, there are also no formal penalties where issues of trade secret theft or breaches occur, other than that seeking relief from breach of terms may be outlined in a con-

tract. A typical method used by entities to ensure the protection of their trade secrets is non-compete and/or non-disclosure agreements. Confidential business data can thus be protected using the basic criteria of secrecy and taking reasonable steps to maintain confidentiality.

c) Sui Generis ("Sweat of the Brow") Database Law

Nigeria does not recognize a sui generis database right. There have been calls for the introduction of such rights especially given the value of structured data in sectors like fintech and healthtech in Nigeria, but conversations regarding this have been few and have not led to concrete legislative proposals.

d) Contract Law

Similar to trade secrets, contracts are governed by principles of common law, statutes such as the Sale of Goods Act, and judicial precedents. Parties can negotiate the terms covering the ownership, use, and protection of proprietary or sensitive data as long as it is not contrary to the principles of contracting. Data as an IP asset is often protected via licensing agreements, terms of service, confidentiality, or nondisclosure agreements. These offer some quasi-IP protection. Confidentiality agreements or NDAs, for instance, are widely used to prevent unauthorized disclosure of data, especially when it serves as a trade secret or holds commercial value. However, its effectiveness could be undermined by the principle of privity of contract and contractual protection being inherently limited to the parties involved in the agreement. This means that third parties who were not privy to the contract cannot be held liable for unauthorized use of the data unless separate legal claims are made. This is more of a private protection of data that applies on a case-by-case basis.

e) Consumer Privacy and Data Security Laws

An individual's privacy rights are primarily governed by the Nigeria Data Protection Act (NDPA) 2023, which focuses on the protection of personal data, that is, information that relates to an identifiable individual. The Act guides the lawful processing of personal data, data minimization, and sets out policies that prevent unauthorized access or misuse of consumers' data. Its scope, however, does not extend to the protection of non-personal data or data sets as a proprietary asset. It is incumbent, therefore, to make a distinction between data as personal information, which is accorded protection by legal systems around the globe, and data (including non-personal data) as a commodified, proprietary resource in this context.

f) Other Relevant Legal Bases

(i) The Constitution

Section 37 of the 1999 Constitution guarantees the right to privacy. This includes the privacy of communications, homes, and correspondences. This has been interpreted to also cover data privacy, preventing digital surveillance and telecom data sharing.

(ii) Patent

Generally, it would be difficult to register data as a Patent in Nigeria. This is because patents may only be issued to an actual invention as obtained under the Nigerian Patents and Designs Act 2004. Such an invention must meet the requirements of being novel, resulting from inventive activity, and capable of industrial application. It must also not be excluded from patentability under the Act. Although data-driven innovations like AI-powered or automated systems may be protected if they meet the patentability criteria, it would be difficult to patent the data itself.

(iii) Cybercrime Act 2015

The Cybercrime Act serves as a backbone to protect database infrastructure from cyber threats and unauthorized access. Some of its provisions allude to the protection of proprietary data. Section 6 criminalizes unauthorized access to computer systems or networks for the purpose

of stealing data vital to national security. Section 12 criminalizes theft of incorporeal property, specifically data interference and unlawful taking or appropriation of digital or intangible IP assets.