Rivista di
Diritti Comparati

Authority-Mediated Trade Secrecy in the AI Act: An Example of Functional Constitutionalisation of Transparency?

*Thomas Margoni, Leona King**

TABLE OF CONTENTS: 1. Introduction. – 2. A Targeted Transparency Architecture under Article 53 AI Act: Normative Context. – 3. Trade Secrets as a Conditional Constraint: The Legal Standard under the Trade Secrets Directive. – 4. Authority-Mediated Trade Secrecy: *CK v Dun & Bradstreet*. – 5. The Commission's Template: Promise, Gaps, and Risks of Under Disclosure: From Principle to Practice. – 6. Conclusion: Towards a Principle of Transparency and Mediated-Authority Trade Secrecy

1. *Introduction*

Artificial intelligence (AI) systems increasingly structure access to information, goods, and public services across most aspects of modern life[1]. Their operation often relies on large data-driven models, including large language models (LLMs), whose provenance and composition are often opaque to affected parties[2]. This opacity is not merely technical; it raises questions of accountability, fairness, and the practical ability of individuals and institutions to exercise rights under Union law[3].

---

* Leona King is funded by the Research Foundation – Flanders (FWO) [grant no. 11A0025N]. This article was subjected to double-blind peer review.

[1] Between October 2024 and March 2025, OpenAI's ChatGPT search alone reached 41.3 million average monthly users in the EU – a sign of how deeply embedded these systems are becoming in everyday life, see OpenAI, [EU Digital Services Act (DSA) Monthly Active Recipients](), October 2025, available at *help.openai.com*.

[2] F. Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge (MA), 2015, p. 193 and p. 217.

[3] C. Novelli, M. Taddeo and L. Floridi, *Accountability in Artificial Intelligence: What It Is and How It Works*, in *AI & Society*, vol. 39, 2024, p. 1871 ff.; L. Grozdanovski, *In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law*, in *Common Market Law Review*, vol. 58, 2021, p. 99 ff.; P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, vol. 55, 2018, p. 1143 ff.

The EU Artificial Intelligence Act[4] (AI Act) responds to this threat of opacity with a risk-based approach that embeds transparency into the governance of, among other forms of AI, general-purpose AI (GPAI). While styled as product-safety regulation, the Act also serves broader constitutional objectives grounded in the Charter of Fundamental Rights: notably the freedoms of expression and information, rights to privacy and data protection, good administration and effective remedy, and protections for property and the freedom to conduct a business[5]. These rights intersect each other and may very well collide, particularly when supporting opposite interests, such as in those cases where transparency and confidentiality are both seen, by different agents in the same transaction, as direct emanation of Charter prerogatives[6]. The Act therefore restages a familiar but pressing dilemma: how to reconcile transparency as a condition of accountability and trust with secrecy, or at least confidentiality, as a condition of innovation and competition[7].

This article explores the reach and limits of trade secrecy in relation to the new obligations introduced by the AI Act, showing the sophisticated processes through which it operates as a conditional and reviewable legal entitlement mediating between the interests of confidentiality with those of transparency. As Aplin and others have argued, trade secrecy is inherently limited by competing rights and public interests[8] and recent data governance instruments and case law increasingly subject trade secrecy claims to independent review[9]. On this trajectory, the article proposes that a comparable model of authority-mediated trade secrecy be adopted, or perhaps is already present in some form, in the AI context, enabling a proportionate reconciliation between transparency obligations and trade secret protection.

The analysis focuses on Article 53 AI Act and its disclosure framework for GPAI models. Article 53 establishes a tiered transparency architecture comprising: (a) technical documentation for competent

---

[4] Regulation (EU) 2024/1689, "AI Act" or "AIA".

[5] Recital 48 AI Act.

[6] C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, 2013.

[7] V. Mayer-Schönberger and T. Ramge, *Reinventing Capitalism in the Age of Big Data*, London, 2018.

[8] T. F. Aplin, *The Limits of EU Trade Secret Protection*, in S. Sandeen, C. Rademacher and A. Ohly (eds), *Research Handbook on Information Law and Governance*, Cheltenham, 2020.

[9] E. De Noyette, L. Stähler and T. Margoni, *Data Secrets: The Data Act's New Trade Secrets Framework*, in *IIC – International Review of Intellectual Property and Competition Law*, vol. 56, 2025, p. 984.

authorities; (b) information for downstream integrators; (c) a copyright compliance policy; and (d) a public "sufficiently detailed summary" of training content. This differentiation reflects the Union's embedding principles of transparency and proportionality[10]: sensitive information flows to narrower audiences under confidentiality; information essential to public accountability flows outward. Recital 107 clarifies the objective of the public summary: to enable «parties with legitimate interests, including copyright holders» to exercise and enforce their rights. Article 78, in turn, protects trade secrets but expressly subjects confidentiality to the Trade Secret Directive's (TSD)[11] lawful disclosure and public interest boundaries. Read together, these provisions encode transparency and secrecy as mutually conditioning rights rather than hierarchical absolutes.

This reading is supported by doctrine[12] and recent case law[13]. The TSD protects information only where it is secret, derives commercial value from that secrecy, and is subject to reasonable protective measures, criteria that generally fit structured, bounded know-how rather than diffuse training corpora assembled from public sources. The Directive also recognises lawful disclosure where «required or allowed by Union law» and for the

[10] K. Lenaerts, *Exploring the Limits of the EU Charter of Fundamental Rights*, in *ECLR*, vol. 8, 2012, p. 375; R. Schütze, *European Constitutional Law*, Cambridge, 2021, p. 223–227; G. de Búrca, *The Principle of Proportionality and Its Application in EC Law*, in *Yearbook of European Law*, vol. 13, 1993, p. 105 ff.; G. De Gregorio, *Digital Constitutionalism in Europe*, Cambridge, 2022, p. 262–272.

[11] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (Trade Secrets Directive).

[12] T. F. Aplin, *The Limits of Trade Secret Protection,* cit., p. 1014, p. 1021; E. De Noyette, L. Stähler and T. Margoni, *Data Secrets,* cit., T. F. Aplin, presentation at *"(Re)evaluating Trade Secrets Protection in Light of AI"*, *Centre for Intellectual Property and Information Law Spring Conference*, University of Cambridge, 2025, available at *cipil.law.com.uk*; M. Leistner and L. Antoine, *IPR and the Use of Open Data and Data Sharing Initiatives by Public and Private Actors*, Brussels, 2022; T. F. Aplin, *Trading Data in the Digital Economy: A Trade Secrets Perspective*, in S. Lohsse, R. Schulze and D. Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, 2017, p. 59–72; T. F. Aplin, A. Radauer, M.-A. Bader et al., *The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis*, in *IIC – International Review of Intellectual Property and Competition Law*, vol. 54, 2023, p. 826.

[13] CJEU, 4 May 2023, C-487/21, *Österreichische Datenschutzbehörde and CRIF*, §§ 33, 34 and 39; CJEU, 26 October 2023, C-307/22, *FT (Copies of Medical Records)*, § 73; Opinion of Advocate General Richard de la Tour, 12 September 2024, in Case C-203/22, *CK v Dun & Bradstreet Austria GmbH*, § 45; Opinion of Advocate General Cruz Villalon, 9 July 2015, in Case C-201/14, *Bara*, § 74; Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679*, adopted 29 November 2017, last revised and adopted 11 April 2018, WP260 rev.01, p. 4.

protection of legitimate interests such as textual gateways that accommodate the AI Act's transparency duties. Interestingly, albeit in the different context of personal data protection, in *CK v Dun & Bradstreet (*C-203/22) the Court of Justice rejected blanket invocations of trade secrecy to defeat access rights and required case-by-case, authority-led proportionality review where secrecy is claimed. While the case arises under the GDPR[14], its logic travels: where fundamental rights are engaged, controllers cannot self-certify secrecy to displace transparency.

Against this backdrop, the Commission's 2025 Explanatory Notice and Template[15] for Article 53(1)(d) aims to operationalise the public summary. While guidance and standardisation are welcome, the current design risks a degree of defensive opacity by over-delegating disclosure choices to data holders (providers in the AIA parlance), relying on narrative description, and limiting dataset level identifiability. The result may be formal transparency without functional verifiability, frustrating Recital 107's aim of enabling rightsholders and other parties with legitimate interests to act.

The article proceeds in four steps. Section 2 reconstructs Article 53's tiered transparency architecture and clarifies how the Act differentiates audiences (regulators, downstream integrators, the public) and purposes (oversight, interoperability, accountability). Section 3 supports and further substantiates the claim that trade secrets function as a conditional constraint, not a categorical bar[16], and explains how Articles 53 and 78 incorporate the TSD's lawful disclosure and public interest exemptions in a coherent way. Section 4 develops the idea of authority-mediated trade secrecy as a procedural standard, borrowing from the framing of the CJEU in *CK v Dun & Bradstreet* as well as from scholar analysis in the Data Act[17]. It translates the secrecy-transparency dichotomy into a reviewable process:

---

[14] Regulation (EU) 2016/679 (General Data Protection Regulation).

[15] European Commission, *Explanatory Notice and Template for the Public Summary of Training Content for General-Purpose AI Models*, Brussels, 2025, available at *digital-strategy.ec.europa.eu*.

[16] U.-M. Mylly, *Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information*, in *European Journal of Law and Technology*, vol. 14, 2023, p. 1014; T. F. Aplin, *The Limits of Trade Secret Protection*, cit.; A. Van Caenegem and L. Desaunettes-Barbero, *Trade Secrets and Intellectual Property*, 2nd ed., Cheltenham, 2025.

[17] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, OJ L 2023/2854 (Data Act, DA); see T. Margoni and E. De Noyette, *Bedrijfsgeheimen in de Dataverordening: Een Administratieve Wending*, in *Intellectuele Eigendom en Reclamerecht*, vol. 41, no. 1, 2025, p. 1–4.

the burden lies with providers to substantiate secrecy; competent authorities decide; reasons are recorded and reviewable; and disclosure must remain as full as possible. Section 5 applies this framework to the Commission's Template, identifying where its design under-delivers on Recital 107 requirements and proposes a practical blueprint that reconciles transparency and trade secrecy through a multilayered disclosure framework combining targeted transparency[18] with authority-mediated trade secrecy. By introducing a model of authority-mediated trade secrecy, the proposed blueprint would successfully embed oversight and accountability into the regulatory design of the AI Act, thereby advancing what, in our views, is the Union's broader, yet perhaps implicit, project of *functional constitutionalisation of transparency*.

The conclusions argue that, read through the TSD and informed by the CJEU's approach, the AI Act supports a rebuttable presumption of transparency for information necessary to support legitimate interests and rights enforcement. Secrecy persists, but only when justified by proved necessity and verified by independent authority. This is not a model to dilute innovation incentives; rather, it is to ensure that transparency becomes auditable and effective, not merely declaratory. In that sense, the AI Act offers a template for a governance model in which transparency and trade secrecy are co-managed through proportionate procedures rather than asserted as absolutes.

In this article, "functional constitutionalisation of transparency" refers to the process by which transparency obligations, while not framed as an autonomous Charter right, acquire constitutional force because they function as indispensable preconditions for the exercise of other fundamental rights, including access to information, effective remedy, and freedom of expression. Where transparency serves this enabling function, secrecy cannot operate as a self-certified or categorical exception, but must be justified through proportionate, authority-mediated review.

---

[18] P. Keller and T. F. Aplin, [Reconciling Trade Secrets and AI Public Transparency](), 4 December 2024, available at *ssrn.com* (developing the concept of targeted transparency in the context of AI and data law); F. Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, in *Northwestern University Law Review*, vol. 104, 2010, p. 105 (introducing the notion of qualified transparency); M. E. Kaminski, *Understanding Transparency in Algorithmic Accountability*, in W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge, 2020, ch. 5, p. 121–138; M. Maroni, *Mediated Transparency: The Digital Services Act and the Legitimisation of Platform Power*, in M. Hillebrandt, P. Leino-Sandberg and I. Koivisto (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice*, London, 2023, ch. 16.

2. *A Targeted Transparency Architecture under Article 53 AI Act: Normative Context*

Transparency occupies an increasingly central position in the EU fundamental rights discourse, yet its conceptual and normative foundations remain diffuse. It has been framed as a *principle*, a *right*, a *policy tool*, and a *technique of accountability*[19]. Each form expresses a slightly different logic – procedural fairness in administration, access to data and documents, algorithmic explainability, or market oversight[20]. In this sense, transparency operates less as a single legal obligation than as a context-dependent framework through which competing rights and interests are mediated[21].

Article 53 AI Act forms the structural core of the Regulation's transparency regime with regard to GPAI models. It operationalises several Charter rights, most notably the freedoms of expression and information (Article 11 CFR; Article 10 ECHR), and the rights to good administration and access to information (Articles 41–42 CFR), by imposing positive disclosure obligations on private actors whose activities have public interest effects. At the same time, it safeguards other fundamental rights and freedoms by ensuring that these disclosure obligations remain proportionate and do not extinguish legitimate commercial confidentiality.

Rather than imposing a uniform transparency requirement, Article 53 differentiates the intensity of disclosure according to the audience and purpose of information use. Information flows to regulators, downstream providers, and the public through distinct channels, each governed by a different degree of precision and confidentiality[22]. In parallel, the *General-Purpose AI Code of Practice*[23] – a voluntary instrument developed by independent experts at the request of the European Commission – offers interim guidance to support responsible development and deployment of

[19] A. Buijze, *The Principle of Transparency in EU Law*, Utrecht, 2013, p. 47–53; A. Buijze, *Transparency: The Swiss Knife of EU Law*, in *European Review of Public Law*, vol. 26, no. 3, 2013, p. 1123 ff.

[20] J. Krook, et al., *A Systematic Literature Review of Artificial Intelligence (AI) Transparency Laws in the European Union (EU) and United Kingdom (UK): A Socio-Legal Approach to AI Transparency Governance*, in *AI and Ethics*, vol. 5, 2025, p. 4069; M. D. Cole, et al., *Algorithmic Transparency and Accountability of Digital Services*, Strasbourg, 2023, available at *rm.coe.int*; A. Koene, et al., *A Governance Framework for Algorithmic Accountability and Transparency*, Brussels, 2019, available at *europarl.europa.eu*.

[21] A. Buijze, *Transparency: The Swiss Knife of EU Law*, cit., p. 1123.

[22] U.-M. Mylly, *Transparent AI?*, cit., p. 1014, p. 1021.

[23] European Commission, *General-Purpose AI Code of Practice* (Digital Strategy, 2024), available at *digital-strategy.ec.europa.eu*.

GPAI models in anticipation of the AI Act's entry into force, though its detailed implications fall outside the scope of this paper.

2.1. *Regulatory Disclosure*

The first tier concerns regulatory disclosure to the AI Office and national competent authorities. Under Article 53(1)(a) providers of GPAI models must supply upon request the technical documentation listed in Annex XI. Following a different language, but reaching an arguably equivalent obligation, Article 53(1)(c) requires providers of GPAI to provide their copyright compliance policy to the AI Office in the light of a general duty to collaborate and the monitoring powers of the Office (e.g., Arts. 53(1)(3), 56, 68, 88, 89). Access to these materials is intended to allow regulators to verify conformity *ex ante* and investigate compliance *ex post*. Regulatory transparency thus functions as oversight – enabling administrative review while remaining within a confidential channel protected by Article 78.

2.2. *Downstream Disclosure*

The second tier addresses downstream disclosure between GPAI providers and those integrating the model into AI systems. Article 53(1)(b) requires the provision of «the information and documentation necessary» for compliant integration. Although typically implemented through contractual terms, this duty originates in statute and therefore has a public law character within private relationships.

This horizontal transparency extends accountability through the value chain, allowing system developers to meet their own regulatory duties under the AI Act. It also exemplifies how the Regulation projects public law principles, such as fairness, proportionality, and reason giving, into the sphere of private governance. Yet the obligation is explicitly conditioned by Article 53(7), which reiterates that the sharing of information must not compromise trade secrets or confidential business information. The result is a form of targeted transparency regime: disclosure is mandated, but its scope must be limited to what is strictly necessary for downstream compliance.

2.3. Public Disclosure: The "Sufficiently Detailed Summary"

The third and most visible tier introduces public disclosure through Article 53(1)(d), requiring GPAI providers to make *publicly available* a «sufficiently detailed summary about the content used for training the model». This summary is the only element of proactive transparency directed toward the general public. Its purpose is to render AI development traceable, to enable the exercise of rights, particularly copyright[24], (personal) data protection[25], and non-discrimination claims[26], and to foster trust in the regulatory system.

Recital 107 clarifies the intended equilibrium: to respect legitimate secrecy while ensuring that the summary is «generally comprehensive rather than technically detailed». Providers should identify the «main data collections or sets» used for training, including major public or private databases, and give a narrative account of other sources. This formulation establishes an intermediate standard: the summary must reveal the character and provenance of training data without exposing its specific configuration or internal processing. In other words, the legislator defines transparency by function – a disclosure sufficient to make rights exercisable – rather than by "substance".

The Commission's 2025 Template translates this open-textured obligation into a structured format, distinguishing between publicly available, privately licensed, scraped, and synthetic datasets. The model reflects proportional reasoning: the more public the dataset, the more specific the required disclosure; the more private or confidential, the more general the permitted description. Yet, as later sections argue, this calibration may err on the side of caution, allowing providers to default to generality and thereby diluting the summary's value as an enabler of transparency and of the rights that rely on such transparency in order to be effectively exercised.

[24] On the relationship with copyright and AI act see A. Peukert, *Copyright in the Artificial Intelligence Act – A Primer*, in *GRUR International*, vol. 73, no. 6, June 2024, p. 497 ff.

[25] M. Nisevic, A. Cuypers and J. De Bruyne, *Explainable AI: Can the AI Act and the GDPR Go Out for a Date?*, in *Proceedings of the 2024 International Joint Conference on Neural Networks (IJCNN)*, Yokohama, 2024, p. 1 ff.

[26] F. Lütz, *The AI Act, Gender Equality and Non-Discrimination: What Role for the AI Office?*, in *ERA Forum*, vol. 25, 2024, p. 79 ff.

2.4. *A Model of Tiered Transparency*

Taken together, these three layers compose a tiered or targeted transparency architecture[27]. Each tier serves a different function:

Tier	Primary recipient	Function	Legal basis	Fundamental rights implicated
Regulatory	AI Office / competent authorities	Oversight and enforcement	Arts 53(1)(a), (c), 78	Good administration (Art 41); effective remedy (Art 47); freedom to conduct a business (Art 16); property (Art 17)
Downstream	Integrating providers	Interoperability and compliance	Arts 53(1)(b), (7)	Freedom of the arts and sciences (Art 13); freedom to conduct a business (Art 16).
Public	General public	Accountability and trust	Art 53(1)(d), Rec 107	Freedom of expression (Art 11); access to documents (Art 42); privacy & data protection (Arts 7–8); copyright property (Art 17(2))

Table 1 – Multi-tiered transparency structure under the AI Act (author's own assessment)

As Keller and Aplin observe, contemporary transparency regimes have evolved beyond the undifferentiated "right to know" of Freedom-of-Information (FOI) towards targeted transparency, i.e., disclosures tailored to specific purposes, procedures, and parties, with calibrated interfaces to trade secret claims[28]. Transparency functions meaningfully only when its form and audience are aligned with its underlying accountability objective: disclosure without contextual intelligibility does not ensure oversight or

[27] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit. (arguing for meaningful transparency achieved through targeted and context-specific disclosure mechanisms).

[28] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit.; See related scholarship conceptualising *layered* or *qualified transparency* A. Fung, M. Graham and D. Weil, *Full Disclosure: The Perils and Promise of Transparency*, Cambridge, 2007; M. E. Kaminski, *Understanding Transparency,* cit.; F. Pasquale, *The Black Box Society,* cit.; G. De Gregorio, *Digital Constitutionalism in Europe*, Cambridge, 2022; E. Kosta, *Peeking into the Black Box: Transparency Rights under the GDPR and the AI Act*, in *Computer Law and Security Review*, vol. 52, 2023, article 105819.

fairness[29]. The literature has accordingly emphasised the need for the AI Act to supplement traditional FOI regimes, normally limited to public administrations, with structured, audience-sensitive forms of transparency[30]. Read in this light, the AI Act's Article 53(1)(d)'s requirement of a "sufficiently detailed summary" can be understood as a targeted instrument that enables rights-bearing entities (data subjects, rightsholders, researchers, regulators) without compromising secrecy.

The EU's broader regulatory framework already operationalises targeted transparency through differentiated, context-sensitive access rights. As Keller and Aplin outline[31], this approach manifests across several instruments including Article 15 (right of access) and Article 22 (right to explanation) GDPR[32] as well as the access granted to vetted researchers under Art 40 DSA[33]. The list could be further expanded with the numerous access and portability rights, and their relationship with TS, introduced by the Data Act[34].

However, without mechanisms for independent review of confidentiality claims, the risk is that tiered transparency collapses into self-certified opacity. These tensions between disclosure obligations and the protection of confidential information are not new[35], but the AI Act restages them in the novel context of AI systems and data governance[36]. The following sections therefore examine how trade secrets operate as a conditional constraint and how authority-mediated procedures can ensure that secrecy remains the exception, not the rule.

[29] M. E. Kaminski, *Understanding Transparency,* cit.; P. Keller, *Participatory Accountability at the Dawn of Artificial Intelligence*, Dickson Poon School of Law Legal Studies Research Paper Series, 2019, p. 15–16.

[30] H. P. Olsen, et al., *The Right to Transparency in Public Governance*, in *Digital Government Research*, vol. 5, 2024.

[31] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit.

[32] L. Edwards and M. Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, in *Duke Law and Technology Review*, vol. 16, 2017, p. 18 ff.

[33] M. Maroni, *Mediated Transparency: The Digital Services Act and the Legitimisation of Platform Power*, in M. Hillebrandt, P. Leino-Sandberg and I. Koivisto (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice*, London, 2023.

[34] E. De Noyette, L. Stähler and T. Margoni, *Data Secrets,* cit.

[35] E. A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, in *Iowa Law Review*, vol. 96, 2010, p. 791.

[36] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit.

3. *Trade Secrets as a Conditional Constraint: The Legal Standard under the Trade Secrets Directive*

Trade secrets occupy an intermediate space in EU law. As Desaunettes-Barbero observes, «it is challenging to link [trade secret] protection to the interests safeguarded by specific fundamental rights»[37]. The Trade Secrets Directive[38] (TSD) itself is neutral on any fundamental-rights foundation: its Charter references chiefly ensure it does not restrict freedom of expression and information (Recital 19), rather than asserting a positive fundamental right to secrecy[39]. This textual silence underscores the absence of a settled fundamental rights basis for trade secret protection and, correspondingly, its adaptability within the broader Charter framework.

Scholarly and judicial analysis have linked trade secrecy to different Charter rights depending on context: as a facet of *property* (Article 17 CFR)[40], as privacy-adjacent (Article 7, e.g., *Varec* (C-450/06)[41], or as part of to the *freedom to conduct a business* (Article 16 CFR)[42].

The absence of a clear statutorily defined fundamental-rights anchor makes the balancing of trade secrecy with other Charter rights, such as freedom of expression, access to information, or data protection, particularly complex and invites further research into how proportionality and institutional design might provide coherence across these intersecting

---

[37] L. Desaunettes, *Trade Secrets Legal Protection: From a Comparative Analysis of US and EU Law to a New Model of Understanding*, in *Munich Studies on Innovation and Competition*, no. 19, Munich, 2023, p. 115.

[38] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (Trade Secrets Directive).

[39] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure*, COM (2013) 813 final, 2013/0402 (COD), explanatory memorandum noting that the initiative promotes the rights to property and to conduct a business, incorporates safeguards for the rights of defence and to a fair trial, ensures respect for freedom of expression and information, and recognises the importance of safeguarding the rights to privacy and data protection.

[40] L. Desaunettes, *New Model of Understanding*, cit., p. 115; T. F. Aplin, *The Limits of Trade Secret Protection,* cit.; T. F. Aplin, L. Bently, P. Johnson and S. Malynicz, *Gurry on Breach of Confidence*, 2nd ed., Oxford, 2012, ch. 5.

[41] E. De Noyette, *Rights of Access and Trade Secrets: Conflicting Interests, Carefully Balanced*, 2025, available at *stradalex-com.kuleuven.e-bronnen.be.*

[42] V. Cassiers, *La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires*, in *Journal des Tribunaux*, no. 385, 2017, p. 396; V. Cassiers and A. Strowel, *La directive du 8 juin 2016 sur la protection des secrets d'affaires*, in V. Cassiers (ed.), *Le secret*, Brussels, 2017, p. 89 ff.

regimes, especially in emerging contexts such as AI governance and data access regulation.

Against this broader fundamental rights framing, the TSD provides the positive law framework for determining what qualifies as a protectable secret. Article 2(1) identifies the familiar conditions of a trade secret as information that is: (i) not generally known; (ii) has commercial value because it is secret; and (iii) has been subject to reasonable steps to keep it secret[43].

These cumulative conditions embed proportionality within the concept itself: secrecy protection extends only as far as confidentiality is demonstrably maintained and commercially justified[44]. The Directive also establishes a qualified rather than absolute privilege. Articles 1(2)(b), 3(2), and 5 make clear that lawful disclosure may occur where required or permitted by Union or national law, or to protect a legitimate interest, including whistleblowing, workers' representation, and public interest disclosure, all relevant elements in the case of AI[45]. In effect, the TSD asserts trade secrecy as a conditional entitlement, constrained by higher order legal and societal values[46].

3.1. Trade Secrets in the AI Act

The AI Act incorporates this conditional logic directly. Articles 53(7) and 78(1)(a) require the AI Office, national authorities, and other competent bodies to protect «intellectual property rights and confidential business information or trade secrets, including source code». Article 78 AI Act further qualifies the obligation: it does not apply «in the cases referred to in Article 5 of Directive (EU) 2016/943». By explicitly recalling – *ad abundantiam* – the TSD's exceptions the AI Act reinstates, beyond any possible hermeneutic exercise, the nature of trade secrecy.

Read together, Articles 53 and 78 create a two-step test. First, information may be withheld only where it qualifies as a trade secret within the meaning of the TSD, as recognised in Article 78(1). Second, that

[43] Art. 2(1) Directive (EU) 2016/943 (Trade Secrets Directive).

[44] T. F. Aplin, *The Limits of Trade Secret Protection,* cit.

[45] U.-M. Mylly, *Transparent AI?* cit., p. 1014, p. 1021; T. F. Aplin, *The Limits of Trade Secret Protection,* cit.

[46] A. Ohly, *Jurisdiction and Choice of Law in Trade Secrets Cases: The EU Perspective*, in S. Sandeen, C. Rademacher and A. Ohly (eds), *Research Handbook on Information Law and Governance*, Cheltenham, 2021.

confidentiality is not absolute: Article 53(1)(d) expressly requires providers of general-purpose AI models to «make publicly available a sufficiently detailed summary about the content used for training», while Article 78(1) permits disclosure of trade secrets in the situations referred to in Article 5 TSD, i.e. where required by Union law or for the purpose of protecting a legitimate interest. Recital 107 elaborates the rationale for this balance, clarifying that the public summary aims to «facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under Union law» while still respecting trade secret protection. Confidentiality under the AI Act is therefore reactive: it restricts onward dissemination by authorities (Articles 53(1)(a) and 78(1)) but does not nullify the provider's primary duty to disclose in the first place when Union law so requires, including publicly in specific situations (Article 53(d)).

This design reflects the Union's established method of reconciling openness and secrecy through proportional reasoning, a common approach in access-to-documents jurisprudence[47]. Secrecy is never a self-executing defence; it is an interest that must be balanced against competing rights and assessed in context.

3.2. Definitional Scope and the Likelihood of Trade Secret Qualification

Although the complexity of AI systems raises difficult questions, the prevailing literature suggests that only a limited subset of the underlying information is likely to meet the TSD's definitional threshold in practice[48]. As Aplin observes, trade secrets law presupposes information that is structured, identifiable, and human generated[49].

Though not an explicit condition under Article 2 TSD, identifiability is emerging as a jurisprudential requirement closely linked to the Directive's "reasonable steps" criterion. The EUIPO's 2023 litigation survey[50]

[47] See, e.g., GC, 12 October 2007, Case T-474/04, *Pergan v Commission*; CJEU, 18 July 2017, *Commission v Bavarian Lager*, Case C-213/15 P.

[48] S. K. Sandeen and T. F. Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, in R. Abott (ed.), *Research Handbook on Intellectual Property and Artificial Intelligence*, Cheltenham, 2022, p. 454–456.

[49] T. F. Aplin, presentation at *"(Re)evaluating Trade Secrets Protection in Light of AI"*, *Centre for Intellectual Property and Information Law Spring Conference*, University of Cambridge, 2025, available at *cipil.law.cam.ac.uk*.

[50] European Union Intellectual Property Office, *Trade Secret Litigation Trends in the EU: Report on 2023 Case-Law Developments*, Alicante, 2023, available at *euipo.europa.eu*.

highlights decisions across Member States applying this evidentiary discipline: claims framed at a high level of abstraction e.g. vague or blanket claims such as asserting that "all company information" or "everything discussed" constitutes a trade secret are routinely rejected for lack of precision[51].

This specificity requirement matters for AI. Large training datasets used to train large scale AI models are rarely so bounded. Collections such as Common Crawl or LAION-5B aggregate heterogeneous, publicly available material, much of which lacks the confidentiality or internal coherence necessary to constitute a trade secret. Even where data are curated or (pre-)processed, they often remain too diffuse to qualify as an identifiable "body" of knowledge and are commonly drawn from sources that anyone in the field could access[52]. In these circumstances, the claim that disclosure of a "sufficiently detailed summary" would reveal a trade secret appears legally tenuous.

Perhaps, more than the dataset itself, what may form part of a potential trade secret are the parameters or selection logic developed by the AI developer to identify and extract particular data sources. The precise "recipe" to select those sources (e.g., a set of instructions or algorithms given to a crawler on how to identify data that is believed to be relevant for the purposes), could perhaps more logically represent secret information which has commercial value in reason of its confidentiality, thereby satisfying the criteria of Article2(1) TSD. However, the template does not require disclosure of such instructions or algorithms, but only the resulting datasets. Although one might, in theory, attempt to infer the elements of the selection logic through reverse engineering of the disclosed data, this

[51] Estonian Criminal Case Against K. M., J. K., M. K. and BloomEst OÜ (15 May 2020); German Regional Labour Court of Düsseldorf, docket no. 12 SaGa 4/20 (3 June 2020); Hungarian Supreme Court, Gfv.VII.30.179/2020/4 (21 January 2021), Italian Supreme Court of Cassation, no. 34337 (27 December 2019): as cited in *EUIPO, Trade Secret Litigation Trends in the EU: Report on 2023 Case-Law Developments* (n).; T. F. Aplin and L. Bently, *Gurry on Breach of Confidence*, 3rd ed., Oxford, 2020, ch. 5.

[52] See, especially with respect to data generated by connected devices: J. Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 8, 2017, p. 257–292 https://doi.org/10.2139/ssrn.2862975; J. Drexl, *The (Lack of) Coherence of Data Ownership with the Intellectual Property System*, in N. Bruun, G. B. Dinwoodie, M. Levin and A. Ohly (eds), *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur*, Cambridge, 2021, p. 213–223; J. Drexl, *Data Access and Control in the Era of Connected Devices*, study on behalf of the European Consumer Organisation (BEUC), Brussels, 2018, available at *beuc.eu*.

would rarely meet the threshold for revealing protectable information. The relationship between dataset composition and the underlying selection parameters is neither linear nor transparent: a range of alternative filtering, weighting, or ranking methods could generate comparable outputs. Without insight into the provider's internal infrastructure, any attempt to reconstruct the "recipe" would rely on conjecture rather than demonstrable access. In legal terms, such speculative inference would in all likelihood not make the information "readily accessible" within the meaning of the Directive, nor deprive it of the quality of secrecy. Consequently, while the risk of reverse engineering merits contextual evaluation, the structure of the template, which requires only a high-level, categorical identification of training data rather than detailed work-by-work documentation, substantially limits the likelihood that disclosure under Article 53 would compromise a valid trade secret.

Nevertheless, trade secret law can have a *de facto* categorical effect, since the determination of protection typically occurs *ex post* and through litigation between usually unequally situated parties. The result is an asymmetry of information and power, where dominant actors may use trade secret claims strategically to preserve opacity[53]. Furthermore, certain subsets of training data may satisfy the TSD criteria: proprietary, human-generated datasets compiled for specialised domains (for instance, annotated medical images, industrial schematics, or internal user interaction logs). Where such data have been maintained in confidence, possess commercial value by virtue of their secrecy, and are secured through reasonable measures (contractual restrictions, limited access, technical safeguards), they may legitimately attract trade secret protection. The extent to which this protection should constrain transparency obligations, and how the relative tension is addressed in practice, is examined below Section 4 and in Section 5.

3.3. *Confidential Business Information, Overclaiming, and Emerging "Data Secrets"*

The AI Act's reference to «confidential business information or trade secrets» raises potential definitional ambiguity. As Mylly notes, the two

[53] T. F. Aplin, A. Radauer, M. Bader and N. Searle, *The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis*, in *IIC – International Review of Intellectual Property and Competition Law*, vol. 54, 2023, p. 826, p. 836.

terms are likely used interchangeably, with "confidential business information" serving as a descriptive restatement of the TSD's definition rather than a separate category[54]. Nonetheless, the phrasing risks strategic overclaiming: providers may designate as "confidential" any dataset, annotation method, or data curation workflow, thereby undermining Article 53's transparency function. To maintain coherence, "confidential business information" should be interpreted *ejusdem generis* with the TSD, restricted to information that is genuinely secret, commercially valuable because of that secrecy, and subject to reasonable protection measures.

This problem resonates with a broader conceptual evolution in EU information law: the rise of "data secrets"[55]. Under instruments like the Data Act, trade secrecy increasingly coexists with duties of access, sharing, and oversight. Information may remain confidential yet still be subject to controlled disclosure, mediated by administrative procedures or technical protection measures[56]. What is particularly interesting in the proposed category of data secrets is the role of (national) administrative authorities which must adjudicate cases where a data holder under a Data Act obligation to share data wants to elude this obligation. A prominent "defence" in this situation is the claim that the information under a sharing obligation contains, or constitutes, a trade secret. Whereas different types of sharing obligations lead to different types of assessment, a common element is the fact that the administrative authority will have to decide *prima-facie* the validity of the trade secret (counter-) claim by the data holder. That institutional posture maps neatly onto the authority-mediated model advanced here – and anticipated by Keller & Aplin's recommendation to place independent bodies between private claims to secrecy and public claims to transparency[57].

4. *Authority-Mediated Trade Secrecy:* CK v Dun & Bradstreet

The Court of Justice's recent judgment in *CK v Dun & Bradstreet Austria GmbH* (C-203/22)[58] provides a crucial reference point for understanding how Union law reconciles transparency with trade secret

[54] U.-M. Mylly, *Transparent AI?* cit., p. 1014.
[55] E. De Noyette, L. Stähler and T. Margoni, *Data Secrets,* cit.
[56] Ibid.
[57] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit.
[58] CJEU, 27 February 2024, C-203/22, *CK v Dun & Bradstreet Austria GmbH* (*CK v Dun & Bradstreet*),

protection in data intensive contexts[59]. The case concerned an individual's request for access under Article 15(1)(h) of the General Data Protection Regulation (GDPR) to personal data processed by a credit scoring company. The company refused full disclosure, invoking trade secret protection.

The Court, building on prior case law[60], and considering the transparency obligations under Article 12(1) GDPR held that where disclosure might affect trade secret interests, information must still be made available at least to a competent authority or court which then conducts a case-by-case balancing and determines the scope of access in light of the specific circumstances[61]. Importantly, the Court emphasised that such balancing cannot be predetermined by national law: Member States may not enact provisions that automatically give priority to trade secret protection[62].

4.1. *Emerging Principles*

Three strands of reasoning in *CK v Dun & Bradstreet* are particularly relevant for interpreting Articles 53 and 78 AI Act. First, the rejection of blanket confidentiality. The Court affirmed that transparency cannot be displaced by abstract references to business secrecy, reaffirming that «That right [of access] should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property […] However, the result of those considerations should not be a refusal to provide all information to the data subject»[63].

Second, the requirement for independent determination. Only supervisory authorities or courts may decide whether a trade secret claim is valid and whether nondisclosure is proportionate. Private actors may not define for themselves the limits of transparency. This point directly

[59] For review of the case see E. De Noyette, *Rights of Access and Trade Secrets,* cit.

[60] Opinion of Advocate General Richard de la Tour, 12 September 2024, in Case C-203/22*, CK v Dun & Bradstreet Austria GmbH,* cit.; see also ECJ, 7 December 2023, C-634/21, *SCHUFA Holding and Others (Scoring)*; CJEU, 26 October 2023, C-307/22, *FT (Copies from the Medical File),* cit.; and CJEU, 4 May 2023, C-487/21, *Österreichische Datenschutzbehörde and CRIF*, cit.

[61] This case by case recommendation echoes the proposal of G. Malgieri, *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*, in *International Data Privacy Law*, vol. 6, no. 2, May 2016, p. 102 ff.

[62] See *SCHUFA Holding and Others (Scoring)*, C-634/21, ECLI:EU:C:2023:957, § 70 and the case law cited; see also § 75 of the judgment.

[63] Judgment, § 3, citing Recital 63 GDPR.

undermines any reading of the AI Act that would allow providers to unilaterally withhold information under Article 53 on the basis of self-declared confidentiality. At the same time, it paves the way for a much more significant role for the AI Office (and other authorities) in precisely defining this dynamic – a role that these bodies must be willing to embrace[64].

Third, the obligation of intelligibility. Even where some information remains confidential, controllers must provide explanations that are «concise, transparent, intelligible and easily accessible». Complexity or proprietary character cannot nullify the duty to communicate in a form that enables understanding. This requirement of functional comprehensibility should arguably apply *mutatis mutandis* to AI model documentation: summaries must be understandable enough to allow external scrutiny, even if they do not reveal technical detail.

These elements together logically demand a clear procedural standard of proportionality: secrecy claims must be specific, verified and justified, and transparency must remain the rule and confidentiality the exception.

It is important to emphasise that this judicial approach is not confined to data protection law[65]. A comparable model of authority-mediated transparency has long been articulated in EU public procurement case law when trade secrets are invoked. In *Antea Polska* (C-54/21)[66], the CJEU held that contracting authorities may not automatically accept a tenderer's assertion that information constitutes a trade secret. Instead, they must require the economic operator to substantiate the genuinely confidential nature of the information and must themselves conduct an active assessment of whether confidentiality is justified (§ 65). Even where information does qualify as a trade secret, authorities remain under an obligation to disclose the *essential content* of that information in a neutral form, to the extent possible, including through summaries or redacted versions (paras 66–67).

---

[64] T. Margoni and E. De Noyette, *Bedrijfsgeheimen in de Dataverordening: Een Administratieve Wending*, cit.

[65] See also N. Lee, *Governing valuable confidential data in the EU: Transparency as fairness*, in *Improving Intellectual Property*, Cheltenham, 2023, arguing that EU data governance debates extend beyond data protection and reflect broader regulatory and administrative law logics.

[66] CJEU, 28 April 2022, C-54/21, *Antea Polska and Others v Państwowe Gospodarstwo Wodne Wody Polskie (Antea).*

This follows from earlier case law, including *Varec* (C-450/06)[67] and *Klaipėdos* (C-927/19)[68], which similarly requires review bodies and courts to balance the protection of trade secrets against the right to an effective remedy, confirming that confidentiality cannot be permitted to undermine transparency, fair competition, or effective judicial protection. Taken together, this line of jurisprudence reveals an increasingly proceduralised conception of transparency, in which claims to secrecy are subject to verification, balancing, and controlled disclosure under the supervision of public authorities and courts.

4.2. Applying the Standard to the AI Act

The right of access under Article 15 GDPR is instrumental to the effective exercise of other data subject rights, including rectification, erasure, and restriction of processing. Transparency in this context functions not as an end in itself but as a facilitative right, a procedural condition for the realisation of substantive rights[69]. In the *CK* case, the CJEU confirmed that where access may interfere with trade secrets, disclosure must nonetheless occur, if not directly to the data subject, then through a competent authority capable of balancing the rights and interests involved on a case-by-case basis. A similar logic underpins the AI Act's disclosure regime in Article 53 and Recital 107, where transparency is likewise designed to enable the exercise of other Union law rights, such as – but not limited to – those of copyright holders. This elevates transparency to a quasi-constitutional level, one however that is functionally justified (and limited) by the enablement of other fundamental rights. A framework of authority-mediated disclosure provides the mechanism for achieving this balance, ensuring that confidentiality is protected only to the extent strictly necessary and without undermining the rights that transparency is intended to guarantee.

Accordingly, a functionally constitutionalised reading of the transparency requirements of Articles 53 and 78 AI Act in light of the TSD and CJEU case law, suggest a procedural model composed of the following three operational principles:

---

[67] CJEU, 8 November 2007, C-450/06, *Varec SA v Belgian State (Varec)*.

[68] CJEU, 7 September 2021, C-927/19, *Klaipėdos regiono atliekų tvarkymo centras v UAB (Klaipėdos)*.

[69] E. De Noyette, *Rights of Access and Trade Secrets,* cit., p. 144.

a. No automatic exemption – Providers cannot rely on Article 78 to refuse disclosure of the relevant information contained in the "sufficiently detailed summary". They must demonstrate that disclosure would genuinely reveal information satisfying the TSD definition, and that secrecy is necessary. Drawing on Malgieri's notion of decontextualisation developed in relation to personal data, trade secret holders could mitigate disclosure risks by providing context-stripped or abstracted information within the "sufficiently detailed summary"[70]. Such decontextualisation would preserve the informational value necessary for transparency and rights enforcement, allowing verification of data provenance, representativeness, or compliance, while withholding the specific relational or operational details that confer commercial value and constitute the essence of the trade secret.
b. Independent verification – The AI Office or competent national authorities should evaluate each confidentiality claim through a reasoned decision subject to administrative and judicial review.
c. Minimum intelligibility – Even where trade secret protection is upheld, providers must still furnish high level, intelligible information (dataset categories, data sources, timeframes, linguistic coverage) sufficient to allow oversight and the exercise of legitimate interests under Recital 107.

4.3. Constitutionalising Transparency

The *CK* decision and AI Act may therefore reflect a deeper shift in the proper legal categorisation of transparency, namely towards its constitutionalisation. What began as a procedural condition for exercising other rights is increasingly taking on an autonomous constitutional function. This development should not surprise: as public governance, commercial transactions, and even daily life become mediated by data-driven systems, transparency itself becomes a prerequisite for meaningful participation and accountability in the digital order. Transparency has arguably always existed in modern legal frameworks but often only implicitly or embedded in other fundamental rights, such as expression,

[70] G. Malgieri, *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*, cit.

information, and good administration[71]. Yet in an environment that is not merely digital but almost fully "datafied", where the ability to access, understand, and verify information determines the effective enjoyment of many other rights, transparency can no longer remain a secondary or implicit norm. It must be disembedded from its parent rights and recognised as a structural principle of constitutional significance: a form of public accountability appropriate to algorithmic governance.

As a matter of fact, the legislative and judicial trends so far surveyed seem to suggest that transparency may even hold a higher hierarchical position when it conflicts with secrecy, at least when this is due to its function in enabling participation, accountability, and the exercise of other fundamental rights. This fundamental right dimension of transparency, either as an autonomous right or as a necessary enabler of other rights, should, or perhaps must, translate in a rebuttable presumption of transparency to comply with the applicable EU fundamental rights framework. Under this point of view, claims to trade secrecy should be subject to authority-mediated review and sustained only where secrecy is proved as necessary.

Read in light of Articles 53(1)(d) and Recital 107 AI Act, the same presumption should apply to AI training data summaries. Providers must publish information enabling the exercise of legitimate interests under Union law; secrecy may prevail only when independently verified as proportionate. This approach maintains doctrinal coherence with Article 3(2) TSD, which deems lawful any disclosure «required or allowed by Union law», and aligns with broader EU data law trends, particularly the Data Act and the European Health Data Space Regulation[72] (EHDSR), where access to confidential data is permitted under controlled, authority-supervised conditions[73].

To implement this presumption, the AI Office could adopt procedures akin to those of competition and access-to-documents authorities[74]. Accordingly, an argument in favour of the institutionalisation of authority-mediated trade secrecy can be advanced, one in which

[71] P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit.; M. E. Kaminski, *Understanding Transparency*, cit.; A. Buijze, *Transparency: The Swiss Knife of EU Law*, cit.

[72] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance) [2025] OJ L 2025/327 .

[73] E. De Noyette, *Rights of Access and Trade Secrets,* cit.

[74] See Arts. 16–18 of Regulation (EC) No 773/2004; Commission Notice on the Rules for Access to the Commission File in Competition Cases (2005/C 325/07).

independent oversight bodies verify the legitimacy and proportionality of secrecy claims before they restrict disclosure. This proceduralisation would deter overclaiming, foster consistent interpretation, and could support building a *corpus* of soft law clarifying what constitutes a trade secret with respect to training data. Such institutionalisation is indispensable given the danger of an increasingly fragmented governance landscape created by the AI Act, Data Act, EHDSR and related instruments. Coordination among the AI Office, national competent authorities, and related regulators will be essential to ensure coherence and to prevent administrative capacity from becoming the bottleneck of transparency. Without such institutional investment, the Union's promise of balanced openness could risk collapsing into regulatory inertia.

5. *The Commission's Template: Promise, Gaps, and Risks of Under Disclosure: From Principle to Practice*

The Commission's 24 July 2025 Explanatory Notice and Template for the Article 53(1)(d) "sufficiently detailed summary"[75] (hereinafter, referred to as the "Commission's Template") translates an open-textured duty into a standardised disclosure format. This represents a significant institutional advancement, as it aims to enhance comparability and mitigate compliance uncertainty. However, the Template also embodies structural ambivalence. While its tiered design reflects the proportionality logic of the AI Act by calibrating disclosure according to source and sensitivity, it may delegate too much discretion to providers, thereby risking the consolidation of defensive opacity. The central question is whether the mandated disclosures are (i) unlikely to reveal genuine trade secrets under Article 2(1) TSD, and (ii) sufficient to enable «parties with legitimate interests» to exercise their Union law rights (Recital 107). On both counts, the Template may underdeliver.

[75] European Commission, *Explanatory Notice and Template for the Public Summary of Training Content for General-Purpose AI Models*, Brussels, 2025, available at *digital-strategy.ec.europa.eu*.

5.1. *The Template as Institutionalised Transparency?*

The Commission's Template is an important step towards standardising disclosure obligations under the AI Act at an institutional level. Its tiered structure reflects the Regulation's proportionality logic by distinguishing between public, commercial, and proprietary data sources. Yet, while the Template advances comparability and provides greater regulatory certainty, it also delegates substantial discretion to providers, thereby risking the consolidation of defensive opacity, a model in which confidentiality claims expand unchecked, undermining the Act's transparency objective.

From the perspective of balancing trade secrecy and transparency, three dimensions are particularly salient. First, disclosures concerning public and licensed datasets are central to the exercise of legitimate interests, including those of copyright holders under Recital 107. The Template requires identification of the main public or licensed corpora used for training. This obligation should not expose proprietary know-how; rather, it provides provenance information enabling rightsholders to verify lawful text and data mining (TDM) and copyright compliance.

Second, trade secret concerns arise primarily in relation to bespoke or third-party proprietary datasets – namely corpora assembled through targeted collection, annotation, or preprocessing that embed technical or organisational know-how[76].

Third, transparency regarding data processing measures, such as respect for TDM opt-outs and the removal of illegal content, is indispensable for accountability and seems to entail negligible risk to trade secrets. In doing so, the Template focuses on compliance behaviour rather than proprietary techniques, enabling authorities and affected parties to assess whether providers have used data lawfully and mitigated unlawful or biased outputs.

As discussed earlier, what may more plausibly constitute a trade secret in this context are not the datasets themselves, but the selection parameters - the proprietary instructions, algorithms, or criteria used to identify and extract relevant data from public sources. These processes could represent confidential know-how with commercial value by virtue of their secrecy. Crucially, the Template does not require disclosure of such parameters, but

---

[76] A. Nordberg, *Trade Secrets, Big Data and Artificial Intelligence Innovation: A Legal Oxymoron?*, in J. Schovsbo, T. Minssen and T. Riis (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive*, Cheltenham, 2020.

only of the resulting datasets, thereby already excluding the elements most likely to fall within the TSD threshold.

5.2. Proportionality and Legitimate Interest Functionality

While only time (and arguably litigation) will tell, it seems that the current template, while certainly representing a major advancement, probably a unique example of institutionalised transparency tool on a global level, still favours precautionary secrecy over transparency. Measured against Recital 107's functional test, right holders have more information than before to exercise their rights, however, the information contained in the Template is probably not by itself sufficient to enable the exercise and enforcement of all rights or legal entitlements. Building on the logic developed in Section 4, a workable settlement between transparency and confidentiality can be achieved through a targeted transparency framework complemented by authority-mediated trade secrecy. This approach translates the principle of confidentiality into a structured, multilayered disclosure model that aligns with Articles 53 and 78 AI Act. The framework should contain a:

a. Public layer (mandatory): The public layer would contain dataset identifiers for major public and scraped sources, categorical identifiers for licensed corpora, annotated domain lists, language and timeframe metadata, opt-out compliance metrics, and high-level information on user and synthetic data fields. These disclosures pose minimal trade secret risk but are essential to enable rights-holders, data subjects, and regulators to exercise their legitimate interests under Recital 107.
b. Confidential layer (to authorities under Article 78): At the confidential level, providers would submit declarations for each claimed secret, along with sensitive annexes, such as the precise composition of proprietary datasets, lodged for verification rather than publication. This could include controlled access mechanisms such as a secure processing environment (SPE), borrowing the concept from other EU data law, such as the Data Governance Act (DGA) and EHDSR, allowing enhanced inspection by authorities or vetted parties. A comparable logic already exists in trade secret litigation, where *confidentiality clubs* enable limited disclosure of sensitive material to

identified parties under strict non-disclosure conditions[77]. Incorporating a similar procedural safeguard in the AI Act context would preserve confidentiality while ensuring that those with legitimate oversight functions retain effective access for verification and enforcement.

c. Oversight and consistency: The creation of a public registry of anonymised trade secrecy determinations to deter over-claiming and promote convergence in national practice, an approach already proposed in the context of "data secrets"[78]. A comparable registry could serve a similar function under the AI Act, fostering predictability, procedural fairness, and cross-border consistency in the treatment of confidentiality claims. This proportionate implementation model operationalises the presumption of rebuttable transparency discussed earlier. It ensures that trade secrets are protected where necessary yet remain subject to verification through independent authority review. In doing so, it gives concrete effect to the argued Union's broader project of functional constitutionalisation of transparency, embedding oversight and accountability within the digital regulatory order.

6. *Conclusion: Towards a Principle of Transparency and Mediated-Authority Trade Secrecy*

This article has argued that the AI Act establishes a model of targeted transparency in which trade secret protection operates as a conditional and reviewable constraint rather than as an absolute bar to disclosure. Focusing on Article 53 and its tiered disclosure architecture for general-purpose AI models, and read together with Article 78 and Recital 107, the analysis has shown how the Regulation reconciles transparency obligations with trade secret protection through proportional differentiation of audiences, purposes, and levels of detail. Drawing on the TSD and case law, the article has developed the concept of authority-mediated trade secrecy, under which claims to confidentiality must be substantiated, assessed, and, where necessary, limited by independent authorities to ensure that transparency

[77] See, for example, Art. 9 of Directive (EU) 2016/943 (Trade Secrets Directive); E. De Noyette, L. Stähler and T. Margoni, *Data Secrets,* cit.; E. De Noyette, *Rights of Access and Trade Secrets,* cit., p. 139–140.

[78] E. De Noyette, L. Stähler and T. Margoni, *Data Secrets,* cit.

remains effective for the exercise and enforcement of rights under Union law.

By "functional constitutionalisation of transparency", this article does not suggest the emergence of a formally recognised autonomous right to transparency under the Charter. Rather, it describes a process through which transparency begins to operate as a constitutional norm in practice. This occurs where transparency structures relations between private and public actors, conditions the exercise and limitation of fundamental rights, and triggers heightened procedural safeguards. Transparency thus acquires constitutional relevance through function, not formal designation. In this sense, transparency under the AI Act mirrors developments in other areas of EU law, where procedural guarantees increasingly serve as the backbone of rights effectiveness in data-intensive and asymmetrical governance environments.

Within this framework, the AI Act mediates between the Charter's information and access rights (e.g., Articles 7, 8, 11 and 42 CFR) and the freedoms that may underpin trade secrecy – most notably the freedom to conduct a business (Article 16 CFR) and the right to property (Article 17 CFR). The operative equilibrium lies in Articles 53 and 78, read together with Recital 107 AI Act, which translate transparency into a legal rule: disclose what is necessary to make accountability real, protect only what is necessary to preserve legitimate secrecy.

A broader question emerging from this analysis is whether transparency, long treated as an instrument for the exercise of rights, should now be recognised as a constitutional principle in its own right. The trajectory of privacy, from a "right to be let alone"[79] to a fully articulated human right to private life, illustrates how procedural values can evolve into substantive guarantees in line with technological evolution. In the digital age, a context specific "right to know" may be necessary to counterbalance the concentration of informational power within private infrastructures of algorithmic governance[80]. Transparency may therefore be undergoing a

---

[79] S. D. Warren and L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, vol. 4, 1890, p. 193.

[80] The concept of a "right to know" has been more extensively developed in US scholarship: M. Schudson, *The Rise of the Right to Know: Politics and the Culture of Transparency, 1945–1975*, Cambridge (MA), 2015; L. Watson, *The Right to Know: Epistemic Rights and Why We Need Them*, London, 2021; A. Florini (ed.), *The Right to Know: Transparency for an Open World*, New York, 2007. For a recent UK v. EU comparison, see P. Keller and T. F. Aplin, *Reconciling Trade Secrets and AI,* cit. In the EU context, see U.-M. Mylly, *Transparent AI?*, cit.,

comparable transformation, one that warrants further conceptual and doctrinal exploration.

It may be argued that within a framework of digital constitutionalism[81], transparency would operate both as a necessary mechanism of oversight as well as a mode of participation[82]. It would enable independent verification, informed public scrutiny, and accountability. Yet transparency must be substantive rather than merely symbolic. The economic and technological concentration that characterise the current AI landscape may very well confine transparency to a mere formal requirement – another box to tick. The authority-mediated architecture advanced in this article offers an argumentative, and partly interpretative, pathway for rendering transparency effective in practice rather than nominal in form.

For rights to have effective meaning, they must be capable of being exercised. Transparency often serves as a precondition for that exercise. This reasoning, which appears in both CJEU[83] and ECtHR[84] jurisprudence, positions transparency as a functional requirement for the enjoyment and enforcement of rights, rather than a right in itself. However, as digital

---

p. 1018, noting that the access-to-information dimension of freedom of expression has been recognised in ECtHR case law, e.g. ECtHR, 25 June 2013, app. 48135/06, *Youth Initiative for Human Rights v Serbia*, and ECtHR, 28 November 2013, app. 39534/07, *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v Austria*.

[81] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, vol. 19, 2021, p. 41; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2021; E. Celeste, *Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights*, *REBUILD Centre Working Paper No. 16*, 2024.

[82] M. E. Kaminski, *Understanding Transparency,* cit., p. 121 ff.

[83] CJEU, C-203/22, *CK v Dun & Bradstreet Austria GmbH*, cit.; CJEU, 4 September 2025, C-413/23 P, *Single Resolution Board.* These judgments clarified that pseudonymised data remains personal data from the controller's perspective, thereby triggering transparency obligations at the point of collection. This reinforces the principle that transparency is necessary for fundamental rights to be actionable.

[84] ECtHR, 8 November 2016, app. 18030/11, *Magyar Helsinki Bizottság v Hungary*. The European Court of Human Rights recognised a right of access to public information under Art. 10 ECHR, linking transparency directly to the exercise of freedom of expression. The Court identified criteria for assessing restrictions on access to information, framing transparency as essential for democratic participation; see also D. Voorhoof, *Freedom of Expression in the Digital Environment: How the European Court of Human Rights Has Contributed to the Protection of the Right to Freedom of Expression and Information on the Internet*, in E. Psychogiopoulou and S. de la Sierra (eds), *Digital Media Governance and Supranational Courts: Selected Issues and Insights from the European Judiciary*, Cheltenham, 2022, p. 112 ff.

technologies increasingly mediate access to information, goods, and public services, this instrumental conception may no longer be sufficient.

Two interpretive trajectories can be identified. A maximalist view would recognise a distinct right to transparency as part of a new generation of digital constitutional rights. A minimalist view would treat transparency as a derivative functional principle that gives effect to existing rights. The AI Act occupies a position between these poles. It translates freedom of information and accountability ideals into operational duties for private actors whose systems have public impact effects. In doing so, it contributes to what may be described as a *functional constitutionalisation of transparency.*

The Commission's Template for the "sufficiently detailed summary" represents an important step in operationalising this architecture, but its effectiveness will ultimately depend on whether confidentiality claims are meaningfully scrutinised rather than merely formalized. Finally, the future development of this framework will depend in no small part on judicial interpretation. Just as *CK v Dun & Bradstreet* construes GDPR transparency through a proportionate, case-specific assessment of competing interests, rather than allowing blanket reliance on trade secrecy, so too the CJEU can ensure that Article 78 AI Act is applied as a qualified constraint, not an automatic escape from disclosure. When the inevitable conflicts between disclosure obligations and trade secret claims reach CJEU, the Court should affirm that information disclosure required by Union law cannot constitute misappropriation within the meaning of the TSD. Such a holding would preserve coherence across the Union's data governance framework and cement authority-mediation as the procedural standard for reconciling transparency and confidentiality in data-driven societies.

***

ABSTRACT: This article examines how the EU Artificial Intelligence Act (AI Act) seeks to reconcile transparency obligations with the protection of trade secrets through a multi-layered, regulator-facing disclosure framework centred on Article 53. It argues that the AI Act does not merely accommodate competing interests but participates in an emerging model of *authority-mediated trade secrecy* that is reshaping EU data governance. Across recent legislation – including the Data Act and the European Health Data Space Regulation – trade secret protection is increasingly removed from purely private assertion and litigation, and instead assessed, operationalised, and constrained through administrative procedures and institutional oversight.

Drawing on the EU Trade Secrets Directive, the AI Act, and recent case law of the CJEU (e.g. *CK v Dun & Bradstreet* C-203/22), the article conceptualises authority-mediated trade secrecy as a governance model in which independent authorities are tasked with assessing confidentiality claims. The analysis shows that the AI Act establishes a form of targeted transparency that balances, rather than hierarchises, competing Charter interests, including the rights to information and good administration, and the freedoms of property and to conduct a business through differentiated audiences, purposes, and levels of detail.
The article further contends that, despite this design, the current configuration of Article 53(1)(d) and the Commission's 2025 disclosure template risks entrenching defensive opacity by over-delegating discretion to AI providers. The article concludes that, taken together, this trend can be read as establishing *a principle of functional constitutionalisation of transparency,* whereby transparency obligations, while not framed as an autonomous Charter right, acquire constitutional force because they function as indispensable preconditions for the exercise of other fundamental rights. Interpreted in this way, the AI Act consolidates an ongoing evolution in EU data governance, signalling a shift towards a rebuttable presumption of transparency grounded in procedural safeguards, authority oversight, and institutional accountability.

KEYWORDS: AI Act – trade secrets – transparency – fundamental Rights – AI Office template.

***

Thomas Margoni – Professor, Centre for IT & IP Law (CiTiP), Faculty of Law, KU Leuven, Leuven, Belgium (thomas.margoni@kuleuven.be)

Leona King – FWO fellow, Doctoral Researcher, Centre for IT & IP Law (CiTiP), KU Leuven, Leuven, Belgium (leona.king@kuleuven.be)