



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

AI IN MERGERS & ACQUISITIONS: REGULATORY CHALLENGES UNDER COMPETITION LAW AND DATA PROTECTION LAW

~AFNAN MUNAF QURESHI

ABSTRACT

Artificial intelligence has moved from a peripheral due-diligence tool to a central input in the mergers and acquisitions ("M&A") lifecycle, informing target screening, valuation, synergy modelling, and post-merger integration. This transformation strains two regulatory regimes that were not designed with algorithmic decision-making in mind: competition law, which polices market power and coordination, and data protection law, which governs the lawful processing of personal data. This paper examines how AI-driven M&A activity generates novel risks — including "killer acquisitions" of nascent AI competitors, algorithmic facilitation of tacit collusion, data concentration as a barrier to entry, and non-compliant data transfers during due diligence — and evaluates how competition and data protection authorities in the European Union, the United States, and India have begun to respond. Drawing on the Bundeskartellamt's Facebook decision, the European Commission's Google/Fitbit clearance, the Competition (Amendment) Act, 2023 deal-value threshold in India, the General Data Protection Regulation, and the Digital Personal Data Protection Act, 2023, the paper argues that the doctrinal separation between competition law and data protection law is increasingly untenable in AI-driven transactions, and that convergence — through information-sharing, joint theories of harm, and ex-ante regulation such as the EU Digital Markets Act and AI Act — offers the more coherent regulatory path forward.

Keywords: Artificial Intelligence; Mergers and Acquisitions; Competition Law; Data Protection; Merger Control; Killer Acquisitions; GDPR; Digital Markets Act; Competition Act 2002.

I. INTRODUCTION

Artificial intelligence ("AI") has become deeply embedded in the mechanics of mergers and acquisitions. Investment banks and private equity funds now deploy machine-learning tools to screen thousands of potential targets, natural-language-processing systems to conduct contract review during due diligence, and predictive models to forecast synergies and integration risk.¹ At the same time, AI itself has become the object of the transaction: technology incumbents increasingly acquire AI start-ups, model developers, and proprietary datasets to secure a durable advantage in machine-learning capability. Microsoft's investment in and integration with OpenAI, Google's acquisition of DeepMind, and the wave of "acqui-hires" of small AI teams by large platforms are illustrative of a broader pattern in which the targets of M&A are AI capabilities themselves.²

This dual role of AI — as both a tool used in transactions and a target of transactions — creates friction with two distinct but increasingly overlapping bodies of law. Competition law, historically calibrated to detect horizontal overlaps, price effects, and market concentration through asset- or turnover-based thresholds, struggles to capture acquisitions of nascent AI firms with negligible revenue but significant potential to disrupt incumbents. Data protection law, calibrated to individual consent and purpose limitation, struggles to regulate the aggregation of personal datasets that AI-driven due diligence and post-merger integration make newly exploitable at scale. This paper argues that AI-driven M&A exposes a structural gap between these regimes and examines the extent to which regulators in the European Union, the United States, and India have begun to close that gap.

Part II outlines the ways in which AI is transforming the M&A process and the transactions it produces. Part III examines the competition law challenges, including sub-threshold "killer acquisitions," data as a barrier to entry, and algorithmic collusion risk. Part IV examines data protection law challenges arising at the due diligence, signing, and integration stages of a transaction. Part V analyses the convergence of competition and data protection law through

¹See generally McKinsey & Co., *The State of AI in 2023: Generative AI's Breakout Year* (Aug. 2023); Deloitte, *The Case for AI in M&A Due Diligence* (2023).

²See, e.g., Press Release, European Comm'n, *Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions* (Dec. 17, 2020) (illustrating regulatory concern over data-and-technology-driven acquisitions by dominant digital platforms).

case studies, principally the German Facebook proceedings and the EU Google/Fitbit merger clearance. Part VI offers recommendations, and Part VII concludes.

II. ARTIFICIAL INTELLIGENCE ACROSS THE M&A LIFECYCLE

AI intervenes at nearly every stage of a transaction. In the pre-deal phase, machine-learning models trained on financial databases, patent filings, and alternative data (such as web-traffic or hiring patterns) are used to identify acquisition targets and to flag companies exhibiting growth trajectories that traditional financial screening would miss.³

During due diligence, natural-language-processing tools review thousands of contracts, employment agreements, and regulatory filings for red flags in a fraction of the time required for manual review, while predictive analytics models simulate the effect of alternative deal structures on post-merger cash flow. This is also the stage at which AI intersects most directly with data protection law: due diligence data rooms increasingly contain, and AI systems increasingly process, personal data relating to employees, customers, and counterparties of the target, raising questions of lawful basis, purpose limitation, and cross-border transfer that are examined in Part IV.

Post-completion, AI is used for integration planning, including workforce analytics used to plan redundancies and customer-relationship-management data used to cross-sell products across the combined entity's customer base. Each of these uses depends on combining datasets that were previously held separately — the very act that both competition authorities (concerned with concentration of a competitively significant resource) and data protection authorities (concerned with purpose limitation and further processing) are designed to scrutinize.⁴

III. COMPETITION LAW CHALLENGES

A. Sub-Threshold "Killer Acquisitions" of Nascent AI Competitors

Conventional merger control regimes trigger notification obligations based on the turnover or asset value of the merging parties. AI start-ups, however, are frequently acquired at high valuations despite negligible current revenue, because their value lies in proprietary training

³Deloitte, *The Case for AI in M&A Due Diligence* (2023); see also PwC, *AI and the Future of Deal-Making* (2023).

⁴See Wolfgang Kerber, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 9 J. Intell. Prop. Info. Tech. & Elec. Com. L. 310, 316–18 (2018) (discussing data as a competitively significant resource in merger analysis).

data, model architecture, or engineering talent rather than in existing sales.⁵ Such acquisitions can fall below jurisdictional thresholds entirely, escaping merger review even where the acquisition eliminates a nascent competitive threat. Cunningham, Ederer, and Ma coined the term "killer acquisitions" to describe transactions in which an incumbent acquires an innovative target for the purpose of discontinuing the target's competing project; their empirical study of the pharmaceutical sector found that acquired drug projects were less likely to be developed when they overlapped with the acquirer's existing portfolio, and that a conservative 5.3 to 7.4 percent of the acquisitions in their sample fit this pattern, disproportionately occurring just below thresholds for antitrust scrutiny.⁶

The paradigmatic example is not drawn from AI but is nonetheless instructive: in *FTC v. Mallinckrodt ARD Inc.*, the Federal Trade Commission alleged that Questcor Pharmaceuticals (later Mallinckrodt) acquired the United States development rights to Synacthen — a nascent competitor to its ACTH monopoly drug Acthar — not to develop the product but to "thwart a nascent challenge" to its existing monopoly.⁷ The theory of harm — that an incumbent may extinguish a nascent threat before it matures into a genuine competitor — translates directly to the AI sector, where a large platform's acquisition of a small foundation-model developer or a specialized AI tool may forestall competition long before the target generates revenue that would trigger a notification obligation.

B. Data as a Barrier to Entry and Non-Horizontal Theories of Harm

Where an AI acquisition does trigger merger review, the relevant theory of harm frequently departs from the traditional horizontal-overlap model. Because the performance of AI systems depends on access to large, high-quality training datasets, the acquisition of a data-rich target by a dominant platform can foreclose competitors' access to a competitively significant input even absent any direct product overlap. The European Commission's review of *Google/Fitbit* is the leading illustration. The Commission opened an in-depth Phase II investigation into concerns that Google could use Fitbit's health and fitness data to further personalize Google Ads and foreclose competing advertising providers, and that degraded interoperability between

⁵Colleen Cunningham, Florian Ederer & Song Ma, Killer Acquisitions, 129 J. Pol. Econ. 649, 649–51 (2021).

⁶*Id.* at 650, 652.

⁷Complaint at 3, 8, 12, *FTC v. Mallinckrodt ARD Inc.*, No. 1:17-cv-00120 (D.D.C. filed Jan. 18, 2017). The parties settled for \$100 million. Press Release, FTC, Mallinckrodt Will Pay \$100 Million to Settle FTC, State Charges It Illegally Maintained Its Monopoly of Specialty Drug Used to Treat Infants (Jan. 18, 2017).

Android and third-party wearables could foreclose Fitbit's rivals.⁸ The Commission ultimately cleared the transaction subject to ten-year behavioral commitments, including a data-silo obligation preventing Google from using Fitbit-derived health data in Google Ads, and interoperability commitments preserving third-party access to the Fitbit Web API.⁹

The Commission notably considered, but ultimately dismissed, a further theory that the mere combination of Google's and Fitbit's databases would itself confer a competitive advantage sufficient to foreclose rival digital-health providers.¹⁰ The Commission's reluctance to accept a pure "data concentration" theory of harm on the facts of that case illustrates a broader doctrinal difficulty: competition authorities have not yet settled on a stable framework for treating data — as opposed to market share — as the relevant competitive asset, notwithstanding wide agreement that access to large, proprietary, and continuously refreshed datasets is often the binding constraint on entry into AI-intensive markets.¹¹

C. Algorithmic Collusion and Coordinated Effects

A further competition concern arises not from the merger transaction itself but from the AI systems the merged entity subsequently deploys. Where competing firms adopt similar or shared pricing algorithms — whether independently or as a consequence of consolidation in the market for algorithmic pricing software — the resulting behaviour can converge on supra-competitive prices without any explicit agreement between the firms, a phenomenon commonly termed "algorithmic collusion."¹² A merger between two developers of pricing or matching algorithms used across a horizontal market therefore raises coordinated-effects concerns distinct from, but often overlaid on, the unilateral-effects concerns traditionally assessed in merger review. Because coordinated effects of this kind may only become apparent once the merged algorithm is deployed at scale, ex-ante merger review is a poor instrument for

⁸Case M.9660, Google/Fitbit, Comm'n Decision (Dec. 17, 2020); Press Release, European Comm'n, Mergers: Commission Clears Acquisition of Fitbit by Google, Subject to Conditions, IP/20/2484 (Dec. 17, 2020).

⁹Press Release, European Comm'n, *supra* note 9; see also Google's Fitbit Acquisition Is Cleared by EU with Some Conditions Applied, XDA Developers (Dec. 17, 2020).

¹⁰Press Release, European Comm'n, *supra* note 9.

¹¹Wolfgang Kerber, *supra* note 6, at 316–20; OECD, *Data and Competition* (2016).

¹²OECD, *Algorithms and Collusion: Competition Policy in the Digital Age* (2017).

detecting them, which has led several competition authorities to argue for closer ex-post monitoring of algorithmic pricing conduct alongside conventional merger control.¹³

D. Jurisdictional Responses: Thresholds Recalibrated for the Digital Economy

Recognizing that turnover-based thresholds systematically under-capture digital and AI-driven acquisitions, several jurisdictions have introduced deal-value thresholds. Germany and Austria pioneered value-based notification thresholds in 2017, and India has followed suit. The Competition (Amendment) Act, 2023 introduced a deal-value threshold ("DVT") into Section 5 of the Competition Act, 2002, requiring notification to the Competition Commission of India ("CCI") of any transaction whose value exceeds ₹2,000 crore (approximately US\$238–252 million), provided the target has "substantial business operations in India," irrespective of whether conventional asset or turnover thresholds are met.¹⁴ The Ministry of Corporate Affairs has explained to Parliament that the DVT was designed principally to capture digital and "new-age" market transactions in which the target possesses minimal assets or turnover but significant value attributable to data, technology, and innovation — the precise profile of many AI start-up acquisitions.¹⁵

The European Union has taken a complementary but distinct approach through the Digital Markets Act ("DMA"), which does not alter the EU Merger Regulation's notification thresholds but instead imposes an ex-ante obligation on designated "gatekeepers" to inform the Commission of any intended concentration involving another provider of core platform services or any other digital services, regardless of whether the transaction meets ordinary EU or national merger-notification thresholds.¹⁶ This obligation is designed specifically to give the Commission visibility over precisely the sub-threshold acquisitions that concern scholars of killer acquisitions, including acquisitions of AI-focused targets by designated gatekeepers such as Alphabet, Amazon, Apple, Meta, and Microsoft.¹⁷

¹³See Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* 35–55 (2016).

¹⁴Competition (Amendment) Act, 2023, No. 9 of 2023, § 5 (India), inserting a deal value threshold into §5(a) of the Competition Act, 2002; Competition Commission of India (Combinations) Regulations, 2024; Ministry of Corp. Affairs, Notification (Sept. 9, 2024) (India) (bringing the deal value threshold provisions into force with effect from Sept. 10, 2024).

¹⁵Competition (Amendment) Act, 2023: Shaping Competition Regulation in India, Invest India (2023); Merger Control Regime in India: 2023 Revisions to the Competition Law, India Briefing (Oct. 11, 2023).

¹⁶Regulation 2022/1925, art. 14, 2022 O.J. (L 265) 1 (EU) (Digital Markets Act).

¹⁷See generally Regulation 2022/1925, *supra* note 15, art. 3 (designation of gatekeepers).

In the United States, merger notification remains governed by the Hart-Scott-Rodino Antitrust Improvements Act of 1976, which sets notification thresholds by reference to the size of the transaction and the size of the parties, and substantive review proceeds under Section 7 of the Clayton Act, which prohibits acquisitions whose effect "may be substantially to lessen competition, or to tend to create a monopoly."¹⁸ Unlike India and the EU, the United States has not adopted a deal-value threshold, relying instead on enforcement discretion — exemplified by the Federal Trade Commission's willingness, as in the *Mallinckrodt* matter discussed above, to pursue conduct-based monopolization theories against acquisitions that a pure size-based filter would not have captured.

IV. DATA PROTECTION LAW CHALLENGES

A. Due Diligence and the Lawful Basis Problem

AI-assisted due diligence typically requires the target to disclose, and the acquirer's systems to process, large volumes of personal data relating to employees, customers, and business partners, often before any binding transaction has been agreed. Under the General Data Protection Regulation ("GDPR"), such processing must rest on a lawful basis under Article 6, and the fact that a transaction is commercially significant to the parties does not by itself supply that basis; controllers must generally rely on the "legitimate interests" ground, which requires a documented balancing of the controller's interest in the transaction against the data subject's rights and expectations, and which is markedly weaker where the data subject is an ordinary customer with no relationship to the acquiring entity.¹⁹ Article 5(1)(b) further constrains disclosure through the purpose-limitation principle: personal data collected for one purpose (e.g., service delivery to a customer) cannot automatically be repurposed for due diligence disclosure and subsequent AI-driven analysis without further legal justification.²⁰

In practice, this has driven a market practice of anonymization and pseudonymization of due-diligence datasets prior to disclosure, consistent with long-standing guidance from European data protection authorities that irreversibly anonymized data falls outside the scope of data protection law altogether, while pseudonymized data remains "personal data" and subject to the full weight of GDPR obligations.²¹ AI due-diligence tools complicate this practice because

¹⁸Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a; Clayton Act § 7, 15 U.S.C. § 18.

¹⁹Regulation 2016/679, art. 6(1)(f), 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).

²⁰Regulation 2016/679, *supra* note 19, art. 5(1)(b).

²¹Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216 (2014).

machine-learning models can re-identify individuals from ostensibly anonymized datasets by cross-referencing auxiliary information, undermining the anonymization on which lawful disclosure was premised.²²

B. Consent, Purpose Limitation, and the Digital Personal Data Protection Act, 2023

India's Digital Personal Data Protection Act, 2023 ("DPDP Act") imposes an analogous but textually distinct framework. The Act requires a Data Fiduciary to process personal data either with the Data Principal's free, specific, informed, and unconditional consent, or under one of the enumerated "legitimate uses" in Section 7, and requires that consent be limited to the purpose for which it was given.²³ Because the DPDP Act does not contain a general "legitimate interests" ground comparable to GDPR Article 6(1)(f), an acquirer conducting AI-assisted due diligence on an Indian target's customer database faces a narrower set of lawful bases than its EU counterpart, and must generally either rely on a Section 7 legitimate use or obtain fresh consent — a practical impossibility at the due diligence stage of a confidential transaction.²⁴ The Digital Personal Data Protection Rules, 2025, which operationalize the Act on a phased timeline running through May 2027, further require Data Fiduciaries to issue clear, purpose-specific consent notices and to observe data-minimization and storage-limitation principles that constrain the wholesale transfer of customer databases into an acquirer's AI systems.²⁵

C. Post-Merger Integration and Function Creep

Even where pre-merger due diligence is conducted lawfully, the integration of the target's data into the acquirer's AI systems after completion raises an independent purpose-limitation problem. Customers of the target company ordinarily consented to processing by the target for the target's stated purposes; folding that data into the acquirer's recommendation engines, credit-scoring models, or advertising systems typically constitutes a new and materially different purpose that data protection law does not treat as automatically inherited by the

²²See European Data Protection Board, Guidelines 01/2025 on Pseudonymisation (draft) (discussing re-identification risk from advanced analytics).

²³Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 4, 6–7 (India).

²⁴Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 7 (India) (enumerating legitimate uses, none of which squarely addresses M&A due diligence disclosure).

²⁵Digital Personal Data Protection Rules, 2025 (India); Press Info. Bureau, Government of India, Digital Personal Data Protection (DPDP) Rules, 2025 (Nov. 2025).

acquirer.²⁶ This is precisely the concern that animated the Bundeskartellamt's 2019 proceedings against Facebook, discussed in Part V, and that recurs whenever an AI-driven acquirer seeks to combine previously siloed datasets to train a unified model.

D. Cross-Border Data Transfer in Multinational Transactions

Cross-border M&A frequently requires the transfer of personal data out of the jurisdiction in which it was collected — for instance, to a centralized AI due-diligence platform operated by the acquirer's advisers. Under the GDPR, such transfers require an adequacy decision, standard contractual clauses, or another Chapter V transfer mechanism, and the extraterritorial reach of the DPDP Act's Section 16 (restricting transfers to jurisdictions not notified by the Central Government) imposes a parallel constraint on transfers out of India.²⁷ Where an AI due-diligence platform is hosted in a third country, these transfer restrictions can require restructuring of the due diligence workflow itself — for example, through federated or on-premises deployment of AI models rather than transfer of raw personal data to a centralized cloud service.

V. THE CONVERGENCE OF COMPETITION LAW AND DATA PROTECTION LAW

The clearest illustration of the doctrinal convergence between these two fields is the Bundeskartellamt's 2019 decision against Facebook. The German Federal Cartel Office found that Facebook held a dominant position on the German market for social networks and abused that dominance, contrary to Section 19(1) of the Act Against Restraints of Competition ("GWB"), by conditioning use of its service on users' acceptance of terms permitting Facebook to collect and combine "off-Facebook" data — data generated by users' activity on third-party websites and apps — with their Facebook account data, without adequately voluntary consent.²⁸ Critically, the Bundeskartellamt's theory of exploitative abuse was built directly on an alleged violation of the GDPR's consent standard, reasoning that terms of service which are unlawful under data protection law can simultaneously constitute an abuse of dominance where

²⁶Regulation 2016/679, *supra* note 19, art. 6(4) (factors relevant to compatibility of further processing with the original purpose).

²⁷Regulation 2016/679, *supra* note 19, arts. 44–49; Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 16 (India).

²⁸Bundeskartellamt, Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing 1, 12 (Feb. 15, 2019).

imposed by a dominant undertaking.²⁹ After the Higher Regional Court of Düsseldorf granted interim relief suspending the order, the Federal Court of Justice (Bundesgerichtshof) overturned that suspension in June 2020, confirming with "no doubt" that Facebook was abusing its dominant position, and becoming the first European appellate court to treat excessive data collection as a form of anticompetitive conduct.³⁰

The significance of the Facebook proceedings for AI-driven M&A is that they establish, at least in German law, that a merged or organically dominant entity's data-processing practices are not immune from competition scrutiny merely because they are also regulated by data protection law; the two regimes apply cumulatively rather than in the alternative.³¹ The subsequent preliminary reference to the Court of Justice of the European Union, which confirmed that competition authorities may take account of GDPR compliance as one factor in assessing abuse of dominance, has entrenched this convergence at EU level.³²

The Google/Fitbit clearance discussed in Part III.B is the merger-control counterpart to this convergence: although formally a competition law decision under the EU Merger Regulation, the Commission's remedies package — a data silo separating Fitbit health data from Google's advertising systems, and a user-facing consent mechanism governing further use of that data — is functionally indistinguishable from a data protection compliance programme.³³ This suggests that in AI- and data-intensive mergers, effective merger remedies increasingly require competition authorities to draw on data protection concepts — purpose limitation, data minimization, and user consent — that fall outside their traditional area of expertise, reinforcing the case for closer institutional cooperation between competition and data protection regulators.

²⁹Press Release, Bundeskartellamt, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (Feb. 7, 2019).

³⁰Bundesgerichtshof, Case KVR 69/19 (June 23, 2020) (Facebook interim proceedings); see also *A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook* (Case KVR 69/19), 51 IIC 1006 (2020).

³¹See *Meta v. Bundeskartellamt: Something Old, Something New*, Eur. Papers (2024) (analyzing the interaction of EU competition and data protection law after the Meta decision).

³²Case C-252/21, *Meta Platforms Inc. v. Bundeskartellamt*, ECLI:EU:C:2023:537 (July 4, 2023).

³³Council Regulation 139/2004, 2004 O.J. (L 24) 1 (EC) (EU Merger Regulation); Press Release, European Comm'n, *supra* note 9.

VI. RECOMMENDATIONS

First, jurisdictions that have not yet adopted a deal-value or transaction-value notification threshold should consider doing so, calibrated to avoid over-inclusion of routine acquisitions while capturing the high-valuation, low-revenue profile characteristic of AI start-up acquisitions. India's experience with the Section 5 deal-value threshold, and the accompanying "substantial business operations" filter designed to exclude purely foreign transactions with negligible domestic nexus, offers a workable template that other emerging-market regulators could adapt.³⁴

Second, competition authorities should develop an explicit analytical framework for treating data access as a competitive asset in merger review, comparable to the treatment of intellectual property or physical infrastructure, rather than relying on ad hoc theories of harm developed case by case, as occurred in *Google/Fitbit*. The OECD's early work on data and competition provides a starting point, but a settled framework specific to AI training data — including its scale, quality, exclusivity, and substitutability — remains underdeveloped.³⁵

Third, competition and data protection authorities should formalize information-sharing arrangements of the kind that operated informally between the Bundeskartellamt and the Irish Data Protection Commission during the Facebook proceedings, so that data protection violations identified during a merger review, or competition concerns identified during a data protection investigation, can inform parallel proceedings under the other regime without duplicative fact-finding.³⁶

Fourth, merger remedies in AI- and data-intensive transactions should, where appropriate, adopt the "data silo" model pioneered in *Google/Fitbit*, structurally separating the acquired dataset from the acquirer's existing AI training pipeline for a defined period, rather than relying

³⁴Competition (Amendment) Act, 2023, No. 9 of 2023, § 5 (India); Competition Commission of India (Combinations) Regulations, 2024 (defining "substantial business operations in India").

³⁵OECD, Data and Competition (2016), supra note 12.

³⁶Bundeskartellamt, supra note 22, at 12 (noting that the Bundeskartellamt briefed the Irish Data Protection Commission on the Facebook proceedings).

solely on behavioural non-use commitments that are difficult to monitor once data has been technically combined.³⁷

Fifth, acquirers should be required, as a matter of best practice if not binding law, to conduct a data protection impact assessment as part of AI-assisted due diligence itself, addressing the lawful basis for processing due-diligence data, the risk of re-identification of anonymized datasets by the AI tools used in the review, and the cross-border transfer implications of centralized AI due-diligence platforms.³⁸

VII. Conclusion

Artificial intelligence has reshaped both how mergers and acquisitions are executed and what is acquired in them, and in doing so has exposed structural limitations in competition law and data protection law regimes designed for an earlier era of dealmaking. Turnover-based merger thresholds under-capture high-value, low-revenue AI acquisitions of the kind theorized in the killer-acquisitions literature; established competition doctrine lacks a settled framework for treating training data as a competitive asset; and data protection regimes such as the GDPR and India's DPDP Act constrain the very data flows that AI-assisted due diligence and post-merger integration depend upon. The Bundeskartellamt's Facebook decision and the European Commission's Google/Fitbit clearance demonstrate that regulators are already, in practice, blending competition and data protection analysis to address these gaps, even without a unified statutory framework. India's deal-value threshold and the EU's Digital Markets Act notification obligation for gatekeepers show a parallel legislative trend toward closing the sub-threshold acquisition gap. The coherent regulatory response to AI-driven M&A is unlikely to come from either competition law or data protection law operating alone; it will instead depend on the continued convergence of the two regimes, supported by explicit institutional cooperation, updated notification thresholds, and merger remedies that treat data governance as a first-order competition concern.

³⁷Press Release, European Comm'n, *supra* note 9.

³⁸Cf. Regulation 2016/679, *supra* note 19, art. 35 (data protection impact assessment obligation, by analogy).

TABLE OF AUTHORITIES

Statutes and Regulations

Competition Act, 2002, No. 12 of 2003 (India).

Competition (Amendment) Act, 2023, No. 9 of 2023 (India).

Competition Commission of India (Combinations) Regulations, 2024.

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

Digital Personal Data Protection Rules, 2025 (India).

Clayton Act § 7, 15 U.S.C. § 18.

Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a.

Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).

Council Regulation 139/2004, 2004 O.J. (L 24) 1 (EC) (EU Merger Regulation).

Regulation 2022/1925, 2022 O.J. (L 265) 1 (EU) (Digital Markets Act).

Regulation 2024/1689, 2024 O.J. (L) (EU) (Artificial Intelligence Act).

Act Against Restraints of Competition (GWB) § 19(1) (Ger.).

Cases

Case C-252/21, Meta Platforms Inc. v. Bundeskartellamt, ECLI:EU:C:2023:537 (July 4, 2023).

Bundesgerichtshof, Case KVR 69/19 (June 23, 2020) (Ger.).

Bundeskartellamt, Case Summary: Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing (Feb. 15, 2019).

FTC v. Mallinckrodt ARD Inc., No. 1:17-cv-00120 (D.D.C. filed Jan. 18, 2017).

Case M.9660, Google/Fitbit, Comm'n Decision (Dec. 17, 2020).

Case COMP/M.7217, Facebook/WhatsApp, Comm'n Decision (Oct. 3, 2014).

Secondary Sources

Colleen Cunningham, Florian Ederer & Song Ma, Killer Acquisitions, 129 J. Pol. Econ. 649 (2021).

Ariel Ezrachi & Maurice E. Stucke, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy (2016).

Wolfgang Kerber, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 J. Intell. Prop. Info. Tech. & Elec. Com. L. 310 (2018).

OECD, Algorithms and Collusion: Competition Policy in the Digital Age (2017).

OECD, Data and Competition (2016).

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216 (2014).

European Data Protection Board, Guidelines 01/2025 on Pseudonymisation (draft).

McKinsey & Co., The State of AI in 2023: Generative AI's Breakout Year (Aug. 2023).

Deloitte, The Case for AI in M&A Due Diligence (2023).

PwC, AI and the Future of Deal-Making (2023).

