Journal of Development Studies & Entrepreneurship
Oum el bouaghi university/Algeria
ISSN: 2830–988X/ E-ISSN: 2992-152X
Vol:03--№:02--/December:--2025
pp 01-28

OEB Univ. Publish. Co.

Digital markets act and industry 4.0: Aligning competition policy with cybersecurity

قانون الأسواق الرقمية والثورة الصناعية الرابعة: مواءمة سياسة المنافسة مع الأمن السيبراني

Khaled Khellil[1]

[1]*Oum El Bouaghi University, Algeria, khelil.khaled@univ-oeb.dz*

Received: 16/08/2025 **Accepted:** 25/09/2025 **Published:** 07/12/2025

Abstract:

Industry 4.0's convergence of Internet of Things, Artificial Intelligence and cybersecurity systems increases efficiency while expanding systemic cyber risk. The EU's Digital Markets Act (DMA) alters platform dynamics through interoperability and data-sharing mandates, with important security implications. This study assesses how the DMA's ex-ante regime interacts with Industry 4.0 technologies. Using qualitative analysis of policy texts, literature, and case studies, this study identifies risks and regulatory conflicts.

The findings indicate that the DMA promotes contestability but expands attack surfaces, exposes algorithmic opacity and creates tensions with the General Data Protection Regulation (GDPR). Reliance on gatekeeper self-disclosure and fragmented cross-border supervision weakens incident response and supply-chain resilience.

Keywords: Digital Markets Act, Industry 4.0, Cybersecurity.

JEL Classification: K21, L44.

الملخص:

تؤدي تقاطعات الثورة الصناعية الرابعة؛ لا سيما إنترنت الأشياء والذكاء الاصطناعي وأنظمة الأمن السيبرانية إلى زيادة الكفاءة مع توسيع المخاطر السيبرانية النظامية. يغير قانون الأسواق الرقمية للاتحاد الأوروبي في ديناميكيات المنصات عبر متطلبات التشغيل البيني ومشاركة البيانات، مع آثار أمنية مهمة. تقيم هذه الدراسة كيفية تفاعل النظام الاستباقي لقانون الأسواق الرقمية مع تكنولوجيات الثورة الصناعية الرابعة. باستخدام تحليل نوعي لنصوص السياسيات، الأدبيات، ودراسات حالة، لتحديد المخاطر والصراعات التنظيمية.

تشير النتائج إلى أن قانون الأسواق الرقمية يعزز قابلية المنافسة لكنه يوسع مساحات الهجوم، كما أن الاعتماد على الإفصاح الذاتي للمنصات المحتكرة والإشراف العابر للحدود المجزأ يضعف الاستجابة للحوادث ومرونة سلاسل التوريد.

الكلمات المفتاحية: قانون الأسواق الرقمية، الثورة الصناعية الرابعة، الأمن السيبراني.

تصنيف JEL : K21، L44.

***Corresponding author**: Khaled Khellil, **Email**: khelil.khaled@univ-oeb.dz*

1. INTRODUCTION:

The advent of Industry 4.0 marks a profound transformation of industrial and economic landscapes, driven by the convergence of cyber-physical systems, the Internet of Things (IoT), artificial intelligence (AI), and big data (Lu, 2017). This new digital paradigm promises unprecedented efficiency, customisation, and productivity, but it simultaneously introduces complex security challenges and risks that extend beyond traditional cybersecurity concerns. The increasing interconnectedness of smart factories, supply chains, and digital services creates an expansive attack surface, making digitally-transformed markets vulnerable to a new generation of threats (Liao et al., 2017). In this context, the European Union's Digital Markets Act (DMA) emerges as a critical piece of legislation, designed to curb the power of large online platforms, known as "gatekeepers," and foster fairer, more contestable digital markets (Digital Markets Act 2022/1925, 2022). While the DMA is primarily an antitrust instrument, its ex-ante obligations concerning interoperability, data sharing, and transparency have significant, yet often underappreciated, implications for the security and resilience of the Industry 4.0 ecosystem.

The intersection of Industry 4.0's pervasive digital transformation and the DMA's market-shaping regulations creates a particularly complex environment, especially concerning cybersecurity and the evolution of legislative oversight. Industry 4.0's inherent interconnectedness significantly expands the attack surface, introducing new vulnerabilities such as algorithmic manipulation, data flow risks, and challenges to infrastructure resilience (Masum, 2023). Simultaneously, the DMA's mandates for interoperability and data sharing, while intended to promote competition, can inadvertently introduce security risks by requiring platforms to open tightly integrated ecosystems. This convergence necessitates a thorough examination of how existing and evolving legislative frameworks, particularly the DMA, can effectively navigate and mitigate the inherent security challenges posed by Industry 4.0, ensuring both market contestability and robust digital safety.

This paper addresses the central question of how the DMA's framework for legislative oversight can be leveraged to navigate the unique security challenges posed by Industry 4.0. Specifically, this paper examines the synergies and tensions between competition law and cybersecurity regulation in the context of gatekeeper-dominated markets. To address this question, the following objectives have been established:

- Assess security challenges in Industry 4.0, including algorithmic vulnerabilities, data flow risks, and infrastructure resilience;

- Analyse the DMA's evolution from ex-post to ex-ante regulation, highlighting transparency and coordination;
- Propose policies to expand the DMA's security scope and develop integrated oversight mechanisms.

This study contributes to the existing literature by providing a structured framework for understanding the security implications of competition regulation in the context of Industry 4.0. Unlike previous studies that often treat competition and cybersecurity as separate policy domains, this paper argues for an integrated approach. It provides a basis for policy-makers to move beyond a competition-first mindset and to intentionally align market contestability with robust cyber resilience.

Methods and structure:

This study employs a qualitative analysis approach to examine the intersection of Industry 4.0 technologies and the EU's DMA, with a focus on their combined impact on cybersecurity and legislative oversight. It draws on recent academic literature, policy documents, and regulatory frameworks to define the economic and technological dimensions of Industry 4.0 and outline the DMA's scope and provisions. Security risks such as algorithmic vulnerabilities, data flow threats, and infrastructure resilience challenges are systematically categorised and assessed through case studies, enabling a detailed evaluation of emerging threats in the Industry 4.0 context.

The paper first establishes the transformative effects of Industry 4.0 on market dynamics and security landscapes before analysing the DMA's regulatory mechanisms, gatekeeper obligations, and enforcement strategies. It then explores the tensions and synergies between competitive market regulation and cybersecurity concerns, supported by case studies on algorithmic self-preferencing and mandated data portability. The concluding sections synthesise findings and propose targeted policy recommendations to improve coordination between competition law and cybersecurity governance, ensuring a coherent progression from conceptual foundations to practical regulatory guidance.

2. Background:

2.1 Defining Industry 4.0 and key technologies:

Industry 4.0 signifies the profound integration of advanced digital technologies into industrial manufacturing and processes, leading to the creation of highly interconnected and intelligent systems (Lasi et al., 2014). This paradigm is characterised by the convergence of cyber-physical systems, IoT, cloud computing, cognitive computing, and AI (Lu,

2017). At its core, Industry 4.0 involves large-scale machine-to-machine communication and the extensive use of "smart" objects, ranging from machines and products to sensors and robots. This fundamental shift transforms traditional industrial practices towards increasing automation, enhanced self-monitoring capabilities, and decentralised decision-making, where smart machines can autonomously analyse and diagnose issues without constant human intervention (Klingenberg et al., 2019).

Industry 4.0 is underpinned by key technologies that reshape operations and data exchange. Core pillars include Big Data and data analytics for real-time processing; advanced robotics for task automation; and IoT connecting sensorised devices. Additive manufacturing (3D printing) enables rapid prototyping and customisation, while augmented and virtual reality support industrial training and design (Hermann et al., 2016). Cloud computing supplies scalable compute and storage, and advanced cybersecurity protects interconnected systems. Emerging enablers, including AI (machine learning, deep learning), digital twins, blockchain, 5G, and edge computing, augment connectivity and decentralised processing. AI orchestrates capabilities across robotics and real-time analytics. Collectively these technologies enable continuous information exchange across value chains, producing smart factories that optimise processes, increase efficiency, and personalise production.

2.2 Industry 4.0 technologies and economic institutions:

Industry 4.0 technologies, characterised by the deep integration of cyber-physical systems, the Internet of Things, cloud computing and analytics are fundamentally transforming both how firms compete and how markets are structured. By embedding sensors, connectivity and advanced data-processing capabilities throughout their operations, companies can redesign value chains to emphasise speed, customisation, quality and innovation (Haseeb et al., 2019). As a result, traditional, product-centric business models give way to hybrid offerings in which “servitisation” plays a leading role: physical goods are bundled with digital services and continuously updated software, creating ongoing revenue streams and closer customer relationships. At the same time, production processes become far more flexible, enabling small batch sizes and rapid reconfiguration to meet individualised demand (Stock & Seliger, 2016). These capabilities not only yield efficiency gains and cost reductions, but also accelerate a shift toward a knowledge-driven economy in which data and intellectual capital are the primary sources of value.

Yet the very promise of Industry 4.0 also risks reinforcing market-power imbalances. The upfront investment needed to deploy robotics,

smart machinery, advanced sensors and the cloud, let alone the expertise required to collect, clean and analyse massive data sets can be prohibitively expensive for small and medium-sized enterprises. Uncertainty about the size and timing of returns further deters smaller players, leaving large, well-resourced firms to capture most of the gains. Over time, this investment gap concentrates market power among a handful of incumbents, reducing contestability and raising barriers to entry (Brynjolfsson & McAfee, 2014).

AI and Big Data are at the heart of these dynamics. By leveraging vast troves of usage, production and customer data, AI enables firms to personalise offerings, forecast demand more accurately, optimise pricing dynamically and make strategic decisions with unprecedented speed. Those firms that already command large user bases can harvest ever more data expanding and enriching their datasets, which in turn fuels increasingly sophisticated AI models. This self-reinforcing feedback loop amplifies incumbent advantages: more data begets better algorithms, which beget deeper market insights, which beget even more data. New or smaller rivals, by contrast, struggle to match the scale and richness of these data-driven operations. Industry 4.0 technologies and their economic implications can be summarised as follows:

Table 1. Key Technologies of Industry 4.0 and their economic implications

Technology	Brief Characteristic	Economic Implication
Artificial Intelligence (AI)	Enables systems to learn from data, make intelligent decisions, and automate complex tasks	Enhances data analysis, personalization, demand forecasting, pricing optimization, and decision-making, leading to increased competitiveness and revenue; drives market power and potential monopolization due to data control
Internet of Things (IoT)	Interconnected physical devices with sensors and software for data exchange and automation	Increases productivity, flexibility, and efficiency in manufacturing and supply chains; enables predictive maintenance and real-time tracking
Blockchain	Decentralized, distributed ledger technology for secure and transparent transactions	Facilitates secure data exchange, traceability, and new business models; potential for increased trust and reduced fraud
Edge Computing	Distributed computing paradigm bringing computation and data storage closer to data sources	Reduces latency, improves real-time processing, and enhances data privacy by minimizing data transfer to central clouds
Cloud Computing	On-demand availability of computer system resources over the internet	Provides scalable infrastructure, reduces IT costs, and supports big data analytics and AI applications

Big Data Analytics	Processing and analysis of large, complex datasets to uncover patterns and insights	Drives personalized services, market understanding, and competitive advantage; contributes to data monopolies and market inequality
5G	Fifth generation wireless technology for high-speed, low-latency connectivity	Enables real-time communication for IoT and CPS, critical for autonomous systems and smart factories
Additive Manufacturing (3D Printing)	Builds 3D objects layer-by-layer from digital designs	Facilitates mass customization, reduces material waste, and shortens innovation cycles

Source: compiled by the author

2.3 Emerging security risks in digitally-transformed markets:

The integration of smart technologies in Industry 4.0 brings new and intensified security challenges. Core design principles like decentralisation, virtualisation and transparency drive efficiency but can introduce serious vulnerabilities if not underpinned by expert implementation. Manufacturing, as a critical link in global supply chains handling vast volumes of sensitive data, has become a prime target for cybercriminals. The growing attack surface, created by proliferating interconnected devices and systems, offers attackers more entry points and novel weaknesses, making end-to-end security a persistent concern (Wollschlaeger et al., 2017).

Among the most pressing threats are malware variants, social engineering techniques and advanced persistent threats. Ransomware remains particularly disruptive: by encrypting data and often exfiltrating sensitive information, it can halt entire operations and inflict heavy financial, operational and reputational losses (Najmi et al., 2023). Social engineering exploits human factors, frequently serving as the vector for ransomware deployment or other attacks. Advanced persistent threats pose an even graver danger by enabling prolonged, stealthy intrusions that permit data theft and manipulation of industrial control systems (ICS), with the potential to disrupt production or sabotage critical equipment (Casarosa, 2020). Together, these threats highlight that Industry 4.0's risks stem from both its complex digital infrastructure and the human operators within it, requiring security strategies that combine technical controls with staff awareness and training.

Further vulnerabilities arise from the characteristics of IoT devices and the complexities of cloud and big data environments. Many IoT devices prioritise functionality and interoperability over security, leaving them exposed to exploitation via unsecured connections and weak

protocols (Sicari et al., 2015). Cloud computing and big data analytics introduce challenges related to system availability, data integrity, insufficient standardisation and integration issues, all of which can lead to breaches (Li et al., 2020). The massive data volumes generated by IoT networks and processed by AI systems, alongside the distributed, heterogeneous nature of cloud environments, complicate security management and render traditional perimeter defences inadequate.

3. Results:

3.1 The EU Digital Markets Act: scope and core provisions:

The EU's DMA, which entered into force in November 2022 and became fully applicable in May 2023, represents a significant shift in digital regulation. Instead of relying on traditional ex-post antitrust enforcement, which often proves too slow to address fast-moving digital markets, the DMA adopts an ex-ante approach. The legislation aims to ensure fairer competition and contestability by preemptively regulating the behaviour of a small number of dominant online platforms.

3.1.1 Gatekeeper designation criteria:

The DMA introduces a regulatory framework to identify and oversee dominant online platforms, referred to as "gatekeepers." A company is designated as a gatekeeper if it meets three core qualitative criteria: a significant impact on the internal market, provision of a core platform service (CPS) functioning as a key gateway for business users to reach end-users, and a stable, entrenched market position. These criteria are presumed to be met if quantitative thresholds are fulfilled, including an annual EU turnover of €7.5 billion (or a €75 billion market capitalisation), at least 45 million monthly active end-users, and 10,000 yearly active business users in the EU over the past three financial years (Digital Markets Act 2022/1925, 2022). Major firms like Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft have been designated as gatekeepers, collectively overseeing 22 CPS. The CPSs are presented below:

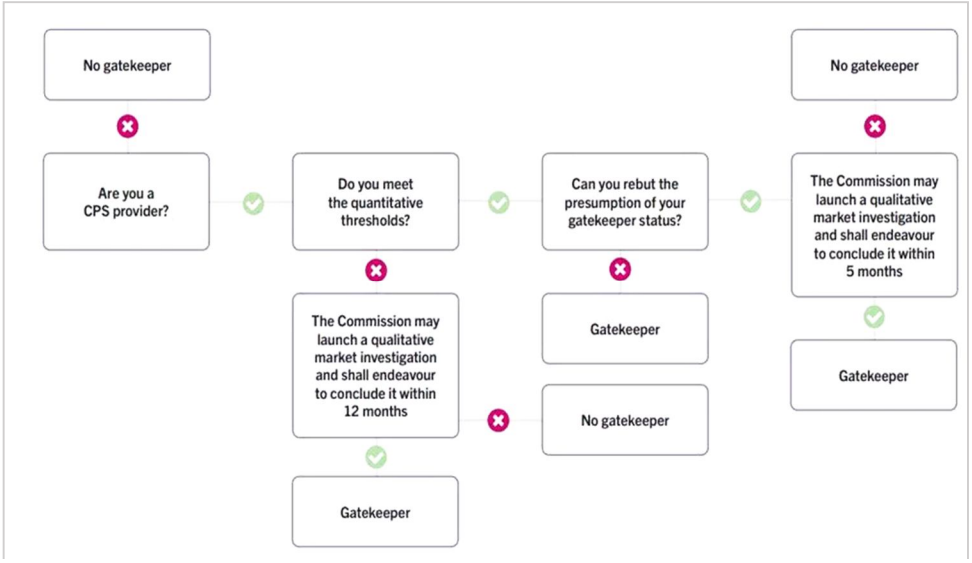
Table 2. Core platform services provided by Gatekeepers

(1) Online intermediation service	**(2) Online search engines**	**(3) Online social networking services**
(4) Video-sharing platform services	**(5) Number-independent interpersonal communications services**	**(6) Operating systems**
(7) Web browsers	**(8) Virtual assistants**	**(9) Cloud computing services**

Note: Online advertising services, advertising exchanges and any other advertising intermediation services provided by a company that provides any of the core platform services listed in points 1- 9
Source: Retrieved from (Linklaters, 2025)

The designation process also allows for qualitative flexibility. Firms that meet the quantitative thresholds may rebut the presumption by providing evidence that exceptional circumstances prevent them from meeting the qualitative criteria. Likewise, the European Commission may designate companies as gatekeepers even if they do not meet the quantitative thresholds, based on a comprehensive market investigation. This flexibility is designed to reduce both type I errors (false positives) and type II errors (false negatives), ensuring that regulation is targeted and proportionate. The Next diagram presents a simplified process of designating gatekeepers (Bostoen & Monti, 2025).

Figure 1. The Designation steps of digital gatekeepers



Source: Retrieved from (Linklaters, 2025)

The DMA includes mechanisms for periodic review, with reassessments required every three years or when material changes occur. While this adaptive approach allows the DMA to remain responsive to technological and market developments, it also introduces legal uncertainty. Firms may face ambiguity about their regulatory status due to the evolving criteria and reliance on qualitative assessments. Moreover, defining the scope and nature of CPSs adds additional economic and legal complexity to the framework. The next table summarises the designation criteria for gatekeepers:

Table 3. DMA Gatekeeper criteria and designated core platform services

Criteria Type	Specific Criteria	Quantitative Thresholds (Presumed Fulfillment)	Examples of Designated Gatekeepers and CPS
Qualitative Criteria (Article 3(1))	Significant impact on the internal market	Annual EU turnover ≥ €7.5 billion (last 3 financial years) OR Average market capitalization ≥ €75 billion (last financial year); AND provides CPS in ≥ 3 Member States	Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft
	Important gateway for business users to reach end-users	CPS has ≥ 45 million monthly active end-users in EU (last financial year); AND ≥ 10,000 yearly active business users in EU (last financial year)	Online intermediation services, Online search engines, Online social networking services, Video-sharing platform services, Number-independent interpersonal communications services, Operating systems, Web browsers, Virtual assistants, Cloud computing services, Online advertising services
	Entrenched and durable position	Met "important gateway" thresholds in each of the last 3 financial years	(Implicitly applies to all designated gatekeepers and their CPS)

Source: By the author based on (Bostoen & Monti, 2025; Digital Markets Act 2022/1925, 2022)

3.1.2 Ex-Ante obligations:

The DMA introduces a proactive regulatory framework targeting large digital platforms, known as gatekeepers, through a defined set of obligations aimed at fostering fair, open, and contestable digital markets. Codified primarily in Articles 5, 6, and 7, these provisions represent a shift from traditional ex-post competition enforcement to ex-ante regulation. Gatekeepers are required to actively demonstrate compliance by submitting detailed implementation reports. This model is intended to expedite enforcement and offer legal certainty by preemptively establishing clear behavioural expectations.

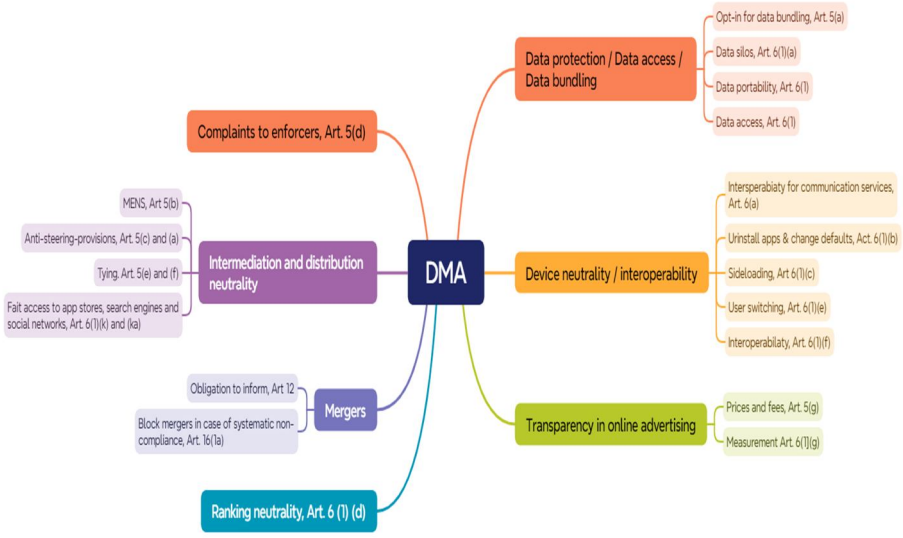
A core focus of the DMA is *interoperability*. Gatekeepers must allow third parties to interact with their CPSs, including permitting the

installation of third-party apps and alternative app stores on their systems. They must also grant equal access to hardware and software functionalities enjoyed by their own services (Digital Markets Act 2022/1925, 2022). This disrupts closed ecosystems by enabling competitors to build on gatekeepers' platforms, with Apple serving as a key example, where access to functionalities such as AirDrop and AirPlay is mandated. These requirements aim to reduce user lock-in, lower entry barriers, and increase consumer choice.

The DMA also imposes extensive *data-sharing* obligations. Gatekeepers are prohibited from merging data across services without explicit, the General Data Protection Regulation (GDPR)-compliant consent from users. They must provide both business and end-users with continuous, high-quality access to data generated on the platform. This goes beyond the GDPR's right to data portability by including both aggregated and non-aggregated data (Digital Markets Act 2022/1925, 2022). These measures are intended to counterbalance gatekeepers' data monopolies, enable effective competition, and empower users to control and move their data across services.

Non-discrimination provisions target self-preferencing practices. Gatekeepers may not favor their own products or services in ranking or presentation over those of third parties. They are also barred from imposing restrictive terms that prevent business users from directing consumers to external offers (Digital Markets Act 2022/1925, 2022). These rules promote fair competition and broader market access for rival firms, ultimately benefiting consumers through improved choice and pricing. In more detail, the obligations can be grouped into 7 themes:

Figure 2: Obligations imposed by the Digital Markets Act



Source: By the author based on (Digital Markets Act 2022/1925, 2022)

The DMA mandates data sharing and interoperability to foster competition, yet these obligations often entail processing personal data. Because the DMA is "without prejudice" to the GDPR, gatekeepers must comply with both regimes, creating tension between DMA-driven access and GDPR principles like explicit consent, purpose limitation, and data minimisation. GDPR-grade consent can impede sharing, letting gatekeepers cite privacy to limit access and weaken contestability (Demircan, 2023). This conflict demands legislative oversight and clear interpretation to reconcile competition and data protection goals.

3.1.3 Enforcement architecture:

The European Commission is the DMA's sole enforcer, empowered to designate gatekeepers, review their status, set obligations, and handle suspension or exemption requests. It oversees submission of annual compliance reports, including audited descriptions of consumer-profiling techniques, investigates non-compliance and circumvention, and conducts market investigations to identify qualifying firms. For systematic breaches it can impose fines up to 10% of global turnover (20% for repeat infringements) and require behavioural or structural remedies. The Commission also dynamically updates gatekeeper obligations and designs targeted remedies (Digital Markets Act 2022/1925, 2022). This centralised

enforcement aims to deliver a consistent, harmonised EU approach and overcome prior cross-border fragmentation.

National Competition Authorities (NCAs) operate alongside the Commission under a cooperative, multi-level enforcement structure. While NCAs may apply Article 102 TFEU and national competition law in parallel with the DMA, coordination mechanisms enshrined in the regulation promote regular exchanges of information with the Commission. NCAs are encouraged to pursue ongoing national cases that overlap with DMA concerns, aiming to secure remedies that mirror DMA-style obligations. Where cases against gatekeepers have a clear national nexus or relate to matters NCAs have previously handled, these authorities may take the lead (Crémer et al., 2023). By combining the Commission's central prerogatives with the NCAs' specialised expertise and local resources, this multi-layered architecture aspires to a more effective and efficient enforcement ecosystem across the Union.

A cornerstone of the DMA's strategy is the requirement for gatekeepers to establish and maintain an internal compliance function. Under Article 28, each gatekeeper must appoint one or more compliance officers; including a head who reports directly to senior management tasked with organising, monitoring, and supervising measures to ensure regulatory adherence. These officers must inform and advise both management and staff on DMA obligations and cooperate with the Commission in its supervisory activities (Colangelo & Martínez, 2025). By embedding *compliance by design* within gatekeeper organisations, this obligation shifts much of the burden of proof to the regulated entities themselves and encourages a proactive culture of legal conformity.

Despite these rigorous reporting requirements, the effectiveness of self-monitoring remains a concern. Initial compliance reports have at times appeared to constitute mere *window dressing*, presenting minor or statutorily required changes as significant DMA-driven reforms. Such superficial disclosures raise doubts about the reports' accuracy and truthfulness and suggest that gatekeepers may seek to circumvent obligations. Indeed, the Commission's early investigations into alleged misreporting by firms such as Apple; launched less than a month after the first reports, underscore the need for active, independent verification. Ensuring genuine compliance will therefore demand robust investigatory follow-through by the Commission beyond reliance on self-reported data.

3.2 Security challenges under Industry 4.0:

3.2.1 Algorithmic vulnerabilities: opacity, bias, manipulation:

The widespread adoption of complex algorithms in Industry 4.0 has introduced critical vulnerabilities, particularly related to opacity, bias, and the risk of manipulation. Advanced algorithms, especially those based on machine learning, are often proprietary and technically opaque, making them difficult to scrutinise or interpret (Shukla, 2025). This lack of transparency conflicts with growing societal and regulatory demands for explainability, especially when such algorithms influence significant decisions. The consequences of this *algorithmic opacity* include delayed detection of harmful outcomes, such as system failures or discriminatory results, which can emerge unexpectedly and with serious ramifications (Lu, 2020).

Algorithmic bias presents another major concern, as it can lead to unjust outcomes and reinforce existing societal inequalities. Bias in AI systems typically stems from flawed design, unrepresentative training data, or the underlying structure of the model. These biases can become embedded in algorithmic processes used in hiring, lending, or access to services, where historical patterns of discrimination are reproduced (Sanclemente, 2023). As algorithms increasingly function as gatekeepers to economic opportunity, they risk entrenching systemic inequalities, influencing who receives employment, credit, or essential services.

In addition to unintentional harms, algorithms are vulnerable to deliberate manipulation, particularly in industrial contexts. Adversarial attacks aim to deceive AI systems by subtly altering input data or interfering with model parameters, leading to inaccurate outputs. Data poisoning is a particularly dangerous tactic, involving the deliberate introduction of misleading information into training datasets to corrupt future decision-making (Olutimehin et al., 2025). These attacks threaten the reliability of critical systems such as autonomous vehicles, intrusion detection, or quality control mechanisms. In smart manufacturing environments, algorithmic manipulation could result in severe operational disruptions, endangering safety and causing substantial financial losses. As AI assumes greater autonomy, securing these systems against manipulation becomes imperative.

The convergence of opacity and bias significantly complicates the issue of accountability. The inability to clearly trace or explain algorithmic decisions undermines efforts to identify responsibility when harm occurs. This is especially problematic in high-stakes areas such as law enforcement, employment, or industrial control, where decisions must be justifiable and auditable (Lu, 2020). The gap between rapid technological

innovation and existing legal and ethical frameworks poses a major challenge for effective regulation, leaving affected individuals with limited recourse and highlighting the urgent need for transparency and governance in algorithmic systems.

3.2.2 Data-flow Risks: breaches, exfiltration, cross-border coordination:

The extensive and continuous data flows inherent in Industry 4.0 and broader digitally transformed markets create significant and pervasive risks of data breaches and exfiltration. Continuous, high-volume data movement across interconnected systems and extensive IoT deployments substantially enlarges the attack surface, increasing susceptibility to data leakage, breaches, ransomware, and data exfiltration (Ramaiah et al., 2022). Ransomware incidents are highlighted as a dual threat: encryption of systems coupled with the prior theft of sensitive information to enhance attackers' leverage. Because every transfer, processing node, and storage endpoint represents a potential vulnerability, comprehensive protection becomes technically complex and operationally persistent (Pedreira et al., 2021).

Cross-border data flows are identified as indispensable to the global digital economy but also as a source of legal and security complexity (OECD, 2022). Data localisation requirements and other restrictions on cross-border movement can produce economic costs and hinder capabilities such as global cybersecurity analytics and fraud prevention, which rely on transnational access to datasets. At the same time, exporting data to jurisdictions with weak security or lax privacy enforcement raises acute compromise risks (Swire & Kennedy-Mayo, 2022). The DMA and its data sharing obligations are discussed in this context: while intended to foster competition, they must be reconciled with GDPR principles, notably consent and purpose limitation, especially for continuous, real-time streams. Secure, GDPR-compliant cross-border data flows therefore depend on balancing economic functionality with privacy and national security, often requiring international cooperation and harmonised legal frameworks (Digital Markets Act 2022/1925, 2022).

The coordination of supervisory responses to cross-border incidents is treated as crucial but procedurally challenging. Under the GDPR, complex cross-border processing incidents invoke a coordination mechanism that designates a lead supervisory authority to manage investigations across Member States. Nevertheless, when individual harms appear negligible, victims are less likely to pursue private legal remedies,

increasing dependence on ex-officio enforcement by Data Protection Authorities (DPAs). Data portability measures, promoted by the DMA to enhance consumer choice, are also problematised: increased portability may improve contestability but concurrently raises questions about ensuring data integrity and safety as information moves between platforms (Zufall & Zingg, 2021).

The DMA mandates data sharing and portability to foster competition in digital markets, increasing the volume and complexity of data flows, including substantial personal data (Hacker et al., 2024). This proliferation expands the attack surface and heightens privacy risks because more data points and transfer mechanisms become potential targets for malicious actors. As a result, a fundamental tension arises between the DMA's goal of promoting market contestability through openness and the GDPR's goal of ensuring robust data protection and privacy. Gatekeepers may exploit this tension by citing GDPR compliance to limit sharing, thereby undermining DMA objectives (Geradin et al., 2022). Addressing this challenge requires a nuanced, integrated regulatory approach.

3.2.3 Infrastructure Resilience: DDoS, supply-chain attacks, cascading failures:

Industry 4.0’s dense coupling of digital infrastructure and physical processes creates acute cybersecurity vulnerabilities that threaten availability, integrity, and safety. The architecture of smart factories and cyber-physical systems relies on pervasive connectivity and heterogeneous IoT endpoints, which expands the attack surface and facilitates large-scale distributed denial of service (DDoS) attacks that can exhaust network and server capacity and deny legitimate access (Hajda et al., 2021). Empirical incidents and industry analyses demonstrate how IoT botnets remain a practical vector for volumetric and amplification DDoS campaigns that materially reduce resource availability and operational reliability in industrial contexts.

Supply chain attacks is a second major vector. The adoption of Supply Chain 4.0 practices, which embed software, firmware, sensors, and third-party services across globally distributed procurement and logistics chains, introduces transitive trust relationships that adversaries can exploit. High-profile software supply chain breaches and managed-service compromises have shown that a single upstream compromise can cascade to thousands of downstream industrial victims, while ransomware campaigns against manufacturers have demonstrated capacity to halt production lines and disrupt critical delivery pipelines (Sobb et al., 2020).

These events underscore the systemic nature of supply chain risk in digitally integrated production ecosystems.

A further concern is cascading failures produced by interdependent critical infrastructures. Cyberattacks targeting one node in an ecosystem can propagate through digital communication links and physical control interconnections to produce disproportionate, non-linear failure modes across energy, transport, and manufacturing sectors. Research on cyber-physical power systems and cascading failure modelling illustrates how localised disturbances may escalate into wide-area outages when shared vulnerabilities and real-time control dependencies are present (Lv et al., 2022). This systemic fragility demands analytic approaches that account for interdependencies and non-linear risk propagation.

Autonomous and decentralised decision-making, central to Industry 4.0's efficiency gains, adds another layer of exposure. Autonomous controllers, real-time analytics, and distributed decision logic depend on trusted data flows and intact control loops. If adversaries disrupt availability, corrupt sensor feeds, or directly manipulate control logic, autonomous systems may execute erroneous or hazardous actions, producing physical damage, safety incidents, or environmental harm beyond conventional data exfiltration (Quezada et al., 2025). Guidance for securing industrial control systems therefore emphasises defence-in-depth across operational technology and ICS components, resilience in control architectures, and supply-chain aware risk management (Fonseca, 2018). The Security challenges discussed can be summarised in the following table:

Table 4. Typology of Industry 4.0 Security Risks

Risk Category	Specific Threat	Description of Threat/Mechanism	Impact
Algorithmic Vulnerabilities	Opacity	Inner workings of complex, proprietary algorithms are incomprehensible, preventing scrutiny.	Difficulty in detecting bias, manipulation, or errors; delayed identification of harmful outcomes; hinders accountability.
	Bias	Algorithmic decisions unjustly favor or disadvantage specific groups due to flawed design or skewed training data.	Perpetuates systemic discrimination in areas like hiring, loan applications, and service access; leads to unfair outcomes.
	Manipulation	Adversarial attacks deceive AI systems by altering input data or	Incorrect predictions, misclassifications, bypassing security

		model parameters; data poisoning corrupts training data.	protocols; systemic failure, sabotage, operational disruptions, safety hazards.
Data-flow Risks	Breaches and Exfiltration	Unauthorised access to, or theft of, sensitive data due to system vulnerabilities or cyberattacks (e.g., ransomware).	Loss of personal information, intellectual property theft, financial losses, reputational damage, operational disruption.
	Cross-border Coordination Challenges	Complexities in managing data security and privacy across different national legal frameworks and enforcement mechanisms.	Economic costs from data localisation, risks from weak foreign security, difficulties in effective supervisory response to incidents.
Infrastructure Resilience	Distributed Denial of Service (DDoS)	Overwhelming networks/servers with traffic to deny service to legitimate users.	Reduced network availability and reliability, operational disruptions, potential damage to industrial installations, safety risks.
	Supply-Chain Attacks	Compromising any link in a digitally-enabled supply chain (software, hardware, logistics).	Widespread operational disruptions, intellectual property theft, sabotage, magnified adverse effects across global networks.
	Cascading Failures	A localised incident or attack propagates through interconnected systems, causing widespread, systemic disruptions.	Systemic outages across multiple industries/critical services, amplified impact of initial disruption, hinders recovery efforts.

Source: Compiled by the author

Taken together, these dynamics indicate that Industry 4.0 requires integrated cybersecurity strategies that combine IoT hardening, supply-chain assurance, systemic resilience and autonomous-control protections to prevent operational disruption and physical risk.

3.3 Case studies:

3.3.1 Case 1: A Gatekeeper's algorithmic recommendation abuse:

Algorithmic self-preferencing by gatekeepers represents a key concern explicitly addressed by the DMA, aiming to prevent dominant platforms from unfairly favoring their own services over those of competitors. The DMA strictly prohibits gatekeepers from treating their own services or products more favorably in ranking or display than similar offerings from third parties on their platforms (Digital Markets Act 2022/1925, 2022). This practice has been a long-standing issue in competition policy, leading to significant antitrust cases against major digital platforms such as Google (involving *Google Shopping*, *Android*, and *AdSense*) and Amazon (concerning its *Buy Box*, *Prime* services, and data utilisation). Self-preferencing allows a gatekeeper to leverage its control over its platform's critical functionalities, such as search results or app store rankings, to gain an undue competitive advantage, thereby distorting competition and limiting consumer choice in the digital marketplace.

The Google Shopping case serves as a prominent example of algorithmic self-preferencing, where a dominant search engine was found to have favored its own comparison-shopping service. In 2017, the European Commission imposed a substantial fine on Google for abusing its market dominance by systematically giving preferential treatment to its own comparison shopping service within its general search results, to the detriment of rival services (European Commission. Joint Research Centre., 2021). This action was explicitly recognised as an abuse of market power by a dominant search engine. This case clearly demonstrated how a gatekeeper's algorithmic design and implementation could directly and significantly impact market outcomes, leading to reduced choice and quality for consumers, despite the theoretical ability of users to switch to alternative services (Tagiuri, 2024a). The DMA's ex-ante prohibition on self-preferencing directly targets such practices, aiming to prevent their occurrence rather than reacting after-market harm has already been inflicted, thereby seeking to establish a more level playing field from the outset.

Implementing the self-preferencing prohibition under the DMA presents inherent challenges, particularly in distinguishing between legitimate product improvements and anti-competitive algorithmic bias. It can be exceptionally difficult to determine the complete absence of self-preferencing and to differentiate it from what might be considered legitimate differential treatment, especially when the ranking or display is

determined by complex, self-learning algorithms (De Streel et al., 2023). The DMA, recognising this complexity, focuses not solely on the welfare effects or efficiencies of such practices, but rather on mandating the explainability of ranking parameters and the design of the consumer interface to minimise inherent platform bias. This approach highlights the intricate nature of regulating algorithmic behaviour, requiring a better understanding of how these algorithms function and how their design choices can impact competition, even if not explicitly intended to be unfair (Tagiuri, 2024a).

The DMA explicitly prohibits algorithmic self-preferencing by gatekeepers (European Commission. Joint Research Centre., 2021). Effective enforcement of this prohibition necessitates a deep understanding of how these complex algorithms rank and display results, as well as how they might be subtly manipulated to favor a gatekeeper's own services (European Commission, 2024). However, a significant obstacle arises from the inherent opacity of many advanced algorithms, often referred to as "black boxes". This opacity makes it exceedingly difficult for regulators to effectively scrutinise and prove instances of self-preferencing (Tagiuri, 2024b). While the DMA mandates transparency on consumer profiling techniques, the actual, intricate workings of complex AI algorithms remain largely hidden. This means it can be challenging to ascertain whether a "self-preferencing" outcome is the result of a deliberate, malicious design choice, an unintended consequence of inherent bias in training data, or a legitimate function aimed at improving user experience or quality (Lu, 2020). This "black box" challenge significantly complicates the burden of proof for regulators and poses an ongoing monitoring challenge for ensuring genuine compliance with the DMA's anti-self-preferencing rules.

3.3.2 Case 2: A cross-border data-portability incident and supervisory response

The DMA mandates data portability as a crucial mechanism to empower users and foster competition within digital markets, yet its implementation intersects with complex data protection requirements, particularly for cross-border data flows. The DMA requires gatekeepers to provide end-users with the ability to port data they have provided or that is generated through their activity on a CPS to other providers, free of charge. This right, while similar to the data portability provisions under the GDPR, extends its scope to include "generated" data and mandates continuous, real-time access to such data (Kubinska et al., 2023). The overarching aim of data portability is to reduce user lock-in to dominant platforms and to ease user acquisition for new market entrants, thereby

stimulating more robust competition in digital markets by enabling a smoother transition of users and their data between services.

The Cambridge Analytica/Facebook data misuse incident, while predating the formal application of the DMA, vividly illustrates the complexities inherent in cross-border data protection failures and the challenges of supervisory response under existing frameworks like GDPR. In this widely publicised case, personal user data, including information from their "friends," was collected without explicit, informed consent through a third-party quiz application and subsequently used for purposes undisclosed to the data subjects. This constituted unlawful data processing and triggered investigations by DPAs in multiple European countries, including the UK, Italy, and Germany (Casarosa, 2020). The incident highlighted a significant failure of the platform to adequately perform its monitoring tasks related to data breaches and the misuse of data by third-party applications integrated into its ecosystem. The Cambridge Analytica affair underscored the profound vulnerability of cross-border data flows to misuse and the persistent difficulties in ensuring user awareness and obtaining valid consent for data processing, particularly when data is collected through indirect means or for purposes not explicitly communicated at the point of collection. Under the GDPR, cross-border data breaches require a lead supervisory authority to coordinate investigations across Member States. However, individually negligible harms discourage private legal action, making enforcement reliant on ex-officio investigations by DPAs. This underscores the enforcement challenges in a globalised digital environment, demanding strong oversight and seamless cross-border cooperation.

While the DMA significantly strengthens data portability obligations, the Cambridge Analytica case underscores potential gaps in proactively preventing data misuse, particularly concerning data generated or collected through third-party applications on gatekeeper platforms. The DMA's Article 5(2) explicitly prohibits gatekeepers from processing personal data from third-party services for online advertising or combining data without the end-user's explicit consent (Digital Markets Act 2022/1925, 2022). It also prohibits "dark patterns" designed to manipulate user consent (European Commission. Joint Research Centre., 2021). Furthermore, gatekeepers are required to submit independently audited reports on their profiling techniques. Had the DMA been in force at the time of the Cambridge Analytica incident, its provisions on explicit consent, restrictions on data combination, and auditing of profiling techniques might have provided a stronger ex-ante framework to prevent

the data harvesting that occurred (Maynard et al., 2022). However, the core issue in the Cambridge Analytica incident revolved around a third-party app's access to and misuse of data. While the DMA's general data sharing principles address gatekeeper-to-business user data flow, the challenge remains in ensuring continuous and robust oversight of all third-party applications' data practices on gatekeeper platforms, especially when they collect data directly from end-users for external purposes.

The ongoing tension between the DMA's data sharing mandates and the GDPR's stringent privacy protections remains a critical area for legislative oversight, as vividly illustrated by the complexities of cross-border data incidents. The DMA explicitly states that it is "without prejudice" to the GDPR, meaning gatekeepers are obligated to comply with both regulatory frameworks simultaneously. This dual requirement can lead to significant regulatory and technical challenges for compliance. Gatekeepers may, for instance, cite GDPR compliance as a legitimate justification for limiting data sharing, potentially creating friction with the DMA's objectives of fostering competition (Weigl et al., 2023). This inherent tension implies that while the DMA aims to open data flows for competitive purposes, the supervisory response to incidents similar to Cambridge Analytica would still heavily rely on the nuanced interpretation and robust enforcement of GDPR's consent and data protection principles (Kubinska et al., 2023). This highlights the persistent need for closer coordination and clearer guidance between competition and DPAs to navigate these complex interdependencies effectively.

The Cambridge Analytica case involved a third-party application misusing data obtained through a gatekeeper platform. Although the DMA addresses gatekeeper obligations and mandates sharing profiling information, its transparency and audit requirements concentrate on gatekeepers' profiling and advertising practices rather than on third-party integrations. The DMA does not explicitly require comprehensive security audits of third-party data handling or continuous monitoring of application access to sensitive user data (Hacker et al., 2024). This regulatory gap suggests the need for mandated security-by-design principles and independent, regular third-party audits for applications interacting with CPSs (Colangelo & Martínez, 2025). Such measures would extend mandatory security assurances across the entire platform ecosystem.

4. Discussion:

This study demonstrates that the DMA, while primarily a competition instrument, materially reshapes the security landscape of Industry 4.0 by forcing openness, interoperability, and data portability among digitally integrated actors. These ex-ante obligations address market concentration and lock-in, but they also enlarge the system-wide attack surface in ways that the DMA's present formulation does not fully anticipate. The paper's case studies and synthesis reveal three interrelated tensions that demand regulatory attention: first, opening platform ecosystems increases opportunities for innovation and competition, yet those same mechanisms create new vectors for supply-chain compromise and data leakage; second, the DMA's demand for transparency confronts the opacity of advanced algorithmic systems, complicating enforcement of anti-self-preferencing rules; third, the protection of commercially sensitive information in competition procedures clashes with the operational need for rapid cyber threat intelligence sharing across public and private actors. These tensions are not hypothetical, they are intrinsic to the convergence of market-shaping rules with cyber-physical systems in manufacturing and logistics, and they require policy responses that explicitly treat safety as a co-equal objective alongside contestability.

A further practical problem is institutional capacity. The DMA centralises enforcement at the European Commission while expecting national competition authorities to cooperate. In practice, coordinating fast-moving security incidents across agencies and Member States exposes procedural frictions, mismatched data taxonomies, and divergent mandates that slow responses and create regulatory arbitrage. The current compliance architecture; reliant on gatekeeper self-disclosure and internal compliance officers creates a risk of "compliance theatre" unless reporting is paired with robust, independent verification and with channels that convert reported incidents into timely, actionable intelligence for cybersecurity authorities. Early Commission probes into alleged misreporting illustrate that self-disclosure alone will not suffice to secure Industry 4.0 critical infrastructures.

Finally, the interplay between DMA obligations and the GDPR generates a practical bind. Gatekeepers may cite data-protection constraints to resist data-sharing obligations, producing friction that can both undermine the DMA's competitive goals and impede coherent security responses. Resolving this tension requires granular legal guidance and technical standards that allow data portability and interoperability to proceed in a manner that is demonstrably privacy-preserving. Without

such clarity, legal uncertainty will be exploited either to restrict legitimate security collaborations or to justify inadequate safeguards when data leaves a gatekeeper's-controlled environment.

Policy recommendations:

- Harmonised incident reporting; DMA + NIS2 (Directive EU 2022/2555) + Cyber Resilience Act: Require gatekeepers to report incidents that materially affect availability, integrity, or confidentiality of Industry 4.0 services using precise thresholds, timelines, and a secure cross-sector platform for authorities and the Commission;
- Narrow, auditable security exceptions for interoperability: Authorise time-limited, documented exceptions (e.g., blocking unvetted linkouts, mandatory third-party code verification) subject to independent review to prevent misuse to effectively recreate closed ecosystems;
- Create a Digital Safety Council: Issue interpretative guidance on DMA-GDPR interactions, standardise incident taxonomies, and coordinate cross-border responses;
- Safe-harbour and antitrust guidance for threat-intelligence sharing: Define permitted information categories, exclude competitively sensitive data, and provide a legal safe harbour for real threat sharing to enable lawful, rapid cooperation;
- Mandate security-by-design and extend independent audits: Require gatekeepers to demonstrate security-by-design across ecosystems; expand audits to supply-chain risk, third-party vetting, and continuous application programming interface monitoring by accredited independent auditors, with anonymised metrics for regulators;
- Regulatory sandboxes and AI oversight tools: Institutionalise sandboxes for privacy-preserving portability and explainability tools; deploy auditable AI-enabled oversight to process large datasets and prioritise inspections;
- Boost enforcement capacity and fast-track powers: Scale technical teams, enable rapid investigative powers and cross-border evidence protocols, and combine credible penalties with remedial orders and mandatory corrective audits.

These reforms seek to align the DMA's market contestability aims with strong cyber resilience, ensuring compatibility through clearer rules, coordination, and technical standards, thereby reducing Industry 4.0 vulnerabilities while maintaining efforts to dismantle entrenched digital gatekeeping.

5. Conclusion:

This study has explored the intricate relationship between the DMA and the security challenges inherent in Industry 4.0. The study began by analysing the defining features of Industry 4.0 and the economic and security risks it presents, particularly those related to the concentration of market power among digital gatekeepers. The study then delved into the DMA's ex-ante regulatory framework, examining its core provisions on interoperability, data sharing, and transparency. The central thrust of the analysis was to evaluate the synergies and tensions between competition law and cybersecurity, a critical nexus in today's digitally-transformed markets.

The key findings of this study underscore a dual reality: while the DMA's mandates are essential for fostering a fairer digital economy, they also introduce new security considerations that require careful legislative and technical oversight. The study has demonstrated that the DMA's push for open ecosystems, if not managed with a robust security-by-design approach, can expand the attack surface and create new vulnerabilities. The self-reinforcing cycles of data and AI that entrench gatekeepers also centralise risk, making the entire ecosystem more susceptible to systemic security incidents. The study highlighted how issues like algorithmic manipulation and data flow risks are not separate from, but rather intertwined with, the competition concerns the DMA is designed to address.

This study's findings have several key implications for future research. A key area is the practical implementation of the DMA’s security provisions. Future work could conduct empirical case studies to analyse how gatekeepers are balancing their interoperability obligations with their cybersecurity responsibilities. Research could also investigate the effectiveness of the proposed enforcement mechanisms, such as institutional sandboxes and AI-enabled oversight tools, in reducing information asymmetries between regulators and gatekeepers. Finally, a comparative analysis of the DMA with other global legislative efforts, such as the US's approach to platform regulation, could provide valuable insights into best practices for managing the security risks of digitally-transformed markets.

6. Bibliography:

a) Bostoen, F., & Monti, G. (2025). The rhyme and reason of gatekeeper designation under the Digital Markets Act. *Journal of Antitrust Enforcement*, jnae054. https://doi.org/10.1093/jaenfo/jnae054
b) Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies* (p. 306). W. W. Norton & Company.
c) Casarosa, F. (2020). Transnational collective actions for cross-border data protection violations. *Internet Policy Review*. https://doi.org/10.14763/2020.3.1498
d) Colangelo, G., & Martínez, A. R. (2025). The Metrics of the DMA's Success. *European Journal of Risk Regulation*, 1–21. https://doi.org/10.1017/err.2025.4
e) Crémer, J., Dinielli, D., Heidhues, P., Kimmelman, G., Monti, G., Podszun, R., Schnitzer, M., Scott Morton, F., & de Streel, A. (2023). Enforcing the Digital Markets Act: Institutional choices, compliance, and antitrust. *Journal of Antitrust Enforcement*, *11*(3), 315–349. https://doi.org/10.1093/jaenfo/jnad004
f) De Streel, A., BOURREAU, M., MICOVA, S. B., FEASEY, R., FLETCHER, A., KRÄMER, J., Monti, G., & Peitz, M. (2023). Effective and Proportionate Implementation of the DMA. *CERRE*. https://cerre.eu/publications/effective-and-proportionate-implementation-of-the-dma-3/
g) Demircan, M. (2023). The DMA and the GDPR: Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions. In F. Bieker, J. Meyer, S. Pape, I. Schiering, & A. Weich (Eds), *Privacy and Identity Management* (pp. 148–164). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-31971-6_12
h) Digital Markets Act 2022/1925, 265 OJ L (2022). http://data.europa.eu/eli/reg/2022/1925/oj/eng
i) European Commission. (2024). *The Digital Markets Act: Ensuring fair and open digital markets*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
j) European Commission. Joint Research Centre. (2021). *The EU digital markets act: A report from a panel of economic experts*. Publications Office. https://data.europa.eu/doi/10.2760/139337
k) Fonseca, L. (2018). Industry 4.0 and the digital society: Concepts, dimensions and envisioned benefits. *Proceedings of the International Conference on Business Excellence*, *12*, 386–397. https://doi.org/10.2478/picbe-2018-0034
l) Geradin, D., Bania, K., & Karanikioti, T. (2022). The interplay between the Digital Markets Act and the General Data Protection Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4203907
m) Hacker, P., Cordes, J., & Rochon, J. (2024). Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond. *European Journal of Risk Regulation*, *15*(1), 49–86. https://doi.org/10.1017/err.2023.81
n) Hajda, J., Jakuszewski, R., & Ogonowski, S. (2021). Security Challenges in Industry 4.0 PLC Systems. *Applied Sciences*, *11*(21), 9785. https://doi.org/10.3390/app11219785

o) Haseeb, M., Hussain, H. I., Ślusarczyk, B., & Jermsittiparsert, K. (2019). Industry 4.0: A Solution towards Technology Challenges of Sustainable Business Performance. *Social Sciences*, *8*(5), Article 5. https://doi.org/10.3390/socsci8050154

p) Hermann, M., Pentek, T., & Otto, B. (2016). Design Principles for Industrie 4.0 Scenarios. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 3928–3937. https://doi.org/10.1109/HICSS.2016.488

q) Klingenberg, C. O., Borges, M. A. V., & Antunes Jr, J. A. V. (2019). Industry 4.0 as a data-driven paradigm: A systematic literature review on technologies. *Journal of Manufacturing Technology Management*, *32*(3), 570–592. https://doi.org/10.1108/JMTM-09-2018-0325

r) Kubinska, A., Daly, K., Zdzieborska, M., & Wise, B. (2023, January 24). Unpacking Digital Data Laws Across Europe: Addressing the Digital Markets Act. *Data Matters Privacy Blog*. https://datamatters.sidley.com/2023/01/24/unpacking-digital-data-laws-across-europe-addressing-the-digital-markets-act/

s) Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4

t) Li, Y., Yu, M., Xu, M., Yang, J., Sha, D., Liu, Q., & Yang, C. (2020). Big Data and Cloud Computing. In H. Guo, M. F. Goodchild, & A. Annoni (Eds), *Manual of Digital Earth* (pp. 325–355). Springer Singapore. https://doi.org/10.1007/978-981-32-9915-3_9

u) Liao, Y., Deschamps, F., Loures, E. de F. R., & Ramos, L. F. P. (2017). Past, present and future of Industry 4.0—A systematic literature review and research agenda proposal. *International Journal of Production Research*, *55*(12), 3609–3629. https://doi.org/10.1080/00207543.2017.1308576

v) Linklaters. (2025). *The gatekeeper designation | Digital Markets Act (DMA) Hub*. https://www.linklaters.com/en/insights/publications/digital-markets-act/dma-hub/the-gatekeeper-designation

w) Lu, S. (2020). Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence. *Vanderbilt Journal of Entertainment & Technology Law*, *23*(1), 99.

x) Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, *6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

y) Lv, H., Wu, Z., Zhang, X., Jiang, B., & Gao, Q. (2022). Cascading Failure Analysis of Hierarchical Industrial Wireless Sensor Networks under the Impact of Data Overload. *Machines*, *10*(5), 380. https://doi.org/10.3390/machines10050380

z) Masum, R. (2023). *Cyber Security in Smart Manufacturing (Threats, Landscapes Challenges)* (No. arXiv:2304.10180). arXiv. https://doi.org/10.48550/arXiv.2304.10180

aa) Maynard, P., Cooper, D., Ahlborn, C., & Oberschelp de Meneses, A. S. (2022, October 10). The Digital Markets Act for Privacy Professionals. *Inside Privacy*. https://www.insideprivacy.com/european-union-2/the-digital-markets-act-for-privacy-professionals/

bb) Najmi, K. Y., AlZain, M. A., Masud, M., Jhanjhi, N. Z., Al-Amri, J., & Baz, M. (2023). A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability. *Materials Today: Proceedings*, *81*, 377–382. https://doi.org/10.1016/j.matpr.2021.03.417

cc) OECD. (2022). *Cross-border Data Flows: Taking Stock of Key Policies and Initiatives*. OECD Publishing. https://doi.org/10.1787/5031dd97-en

dd) Olutimehin, A., Ajayi, A., Metibemu, O. C., Balogun, A., Oladoyinbo, T., & Olaniyi, O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*, 342. https://doi.org/10.9734/jerr/2025/v27i21413

ee) Pedreira, V., Barros, D., & Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors*, *21*(15), 5189. https://doi.org/10.3390/s21155189

ff) Quezada, L., Hermosilla, I., Fuertes, G., Oddershede, A., Palominos, P., & Vargas, M. (2025). Methodologies for Technology Selection in an Industry 4.0 Environment: A Methodological Analysis Using ProKnow-C. *Technologies*, *13*(8), 325. https://doi.org/10.3390/technologies13080325

gg) Ramaiah, M., Chithanuru, V., Padma, A., & Ravi, V. (2022). A Review of Security Vulnerabilities in Industry 4.0 Application and the Possible Solutions Using Blockchain. In R. Sujatha, G. Prakash, & N. Z. Jhanjhi, *Cyber Security Applications for Industry 4.0* (1st edn, pp. 63–95). Chapman and Hall/CRC. https://doi.org/10.1201/9781003203087-3

hh) Sanclemente, G. L. (2023). Digital Tools: Safeguarding National Security, Cybersecurity, and AI Bias. *CEBRI-Revista: Brazilian Journal of International Affairs*, *7*, 137–155.

ii) Shukla, N. (2025). Investigating AI systems: Examining data and algorithmic bias through hermeneutic reverse engineering. *Frontiers in Communication*, *10*. https://doi.org/10.3389/fcomm.2025.1380252

jj) Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

kk) Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics*, *9*(11), 1864. https://doi.org/10.3390/electronics9111864

ll) Stock, T., & Seliger, G. (2016). Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP*, *40*, 536–541. https://doi.org/10.1016/j.procir.2016.01.129

mm) Swire, P., & Kennedy-Mayo, D. (2022). The Effects of Data Localization on Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4030905

nn) Tagiuri, G. (2024a). *Self-Preferencing Practices and Their Future After the DMA* (pp. 189–225). https://doi.org/10.1007/978-3-031-69678-7_8

oo) Tagiuri, G. (2024b). Self-Preferencing Practices and Their Future After the DMA. In D. V. Popović & R. Kulms (Eds), *Repositioning Platforms in Digital Market Law* (Vol. 15, pp. 189–225). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-69678-7_8

pp) Weigl, L., Barbereau, T., Sedlmeir, J., & Zavolokina, L. (2023). *Mediating the Tension between Data Sharing and Privacy: The Case of DMA and GDPR*. https://doi.org/10.5167/UZH-233008

qq) Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. *IEEE Industrial Electronics Magazine*, *11*(1), 17–27. https://doi.org/10.1109/MIE.2017.2649104

rr) Zufall, F., & Zingg, R. (2021). Data Portability in a Data-Driven World. In C.-F. Lin, S. Peng, & T. Streinz (Eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (pp. 215–234). Cambridge University Press. https://doi.org/10.1017/9781108954006.012