

When Corporate Law Meets the Platform Economy

Flaminia Stârc-Meclejan¹

¹ West University of Timișoara, Faculty of Law, flaminia.starc@e-uvt.ro <https://orcid.org/0009-0003-0713-8694>

Abstract: The rise of the digital economy has profoundly transformed how market actors operate. The model of functioning of these platforms challenges the logic of classical corporate law, which is built around the concept of legal personhood. In the case of platforms, there is often no clear distinction between users, collaborators, and consumers, between the “real” and fiscal headquarters, or between the declared and actual activity. Moreover, their operations are often opaque, relying on algorithms that function without transparency and without meaningful avenues for contestation.

This article analyses to what extent classical corporate law concepts - such as legal personhood, patrimonial autonomy, and limited liability - remain suitable in the era of digital platforms, and what directions for reform are emerging from European Union legislation and case law, as well as doctrinal scholarship.

Keywords: corporate law fictions, digital platforms, electronic legal personhood, algorithmic liability, corporate governance obligations adapted to digital risks.

1. Introduction

The rise of the digital economy has driven a profound structural transformation in the way market actors operate. Digital platforms - such as Uber, Airbnb, or Amazon - can no longer be seen as mere technological interfaces that facilitate the meeting of supply and demand. They have become economic actors capable of shaping behaviour, unilaterally regulating contractual relationships, and exercising algorithmic control over users and collaborators¹.

The operational model of these platforms challenges the logic of classical corporate law, built around the concept of the legal entity - a distinct entity endowed with legal personhood, a registered office, a hierarchical organizational structure, its own assets, and a well-defined corporate purpose. In the case of platforms, there is often no clear distinction between users, collaborators, and consumers, or between declared and actual activity. Moreover, their operations are frequently opaque, based on algorithms functioning without transparency or meaningful avenues for contestation².

This dissociation between legal form and economic reality raises fundamental questions about the effectiveness of current legal regimes. Traditional instruments - whether company registration or liability regulation - prove insufficient to capture the complexity of digital entities that operate in networks, beyond geographic boundaries and centralized logic. Similarly, the legal fiction of the corporate personhood seems inadequate in the face of entities functioning as digital ecosystems, where classical legal roles (shareholder, director, employee) are diluted or even disappear entirely.

In this context, without coherent regulatory adaptation, digital platforms risk operating in a zone of impunity, benefiting from legal separateness without assuming the corresponding responsibilities.

This article seeks to analyse to what extent the classical concepts of corporate law - such as legal personhood, patrimonial autonomy, or limited liability - remain adequate in the era of digital platforms, and which directions for reform are emerging from European Union legislation, case law, and scholarly doctrine.

2. Corporate law fictions and digital platforms

Corporate law has been built on a series of legal fictions designed to simplify and facilitate economic activity. Among the most important are the legal personhood of the company, the separation of company assets from those of its members, limited liability, and the autonomy of the will of the corporation expressed through corporate bodies. These constructs enabled the development of modern capitalism, particularly by reducing risks for investors and facilitating capital mobilization³.

¹ Mouial-Bassilana et al. (2025, pp. 144–148).

² *Ibidem*

³ Barbièri (2021, pp. 51–55) for further discussion on corporate order.

Although artificial by nature, corporate law fictions have been essential for regulating economic relationships in increasingly complex contexts. Legal personhood allowed the company to be treated as a distinct legal subject, capable of entering into contracts, acquiring rights, and assuming obligations independently of the individuals who incorporated it. Asset separation provided a clear framework for risk delineation, protecting investors' personal assets from corporate debts. Limited liability, in turn, encouraged investment by making participation in economic initiatives possible without incurring unlimited risk, while the autonomy of corporate will assured that company decisions are taken through internal mechanisms (general assembly, board of directors), even if shareholders ultimately exercise control⁴.

All these fictions rely on a presumption of correspondence between legal form and economic reality. They function effectively as long as the regulated entities conform to classical organizational logic: existence of a headquarters, identifiable decision-makers, a clearly delineated patrimony, and activities conducted within a determinable regulatory framework. At the same time, they imply an acceptance that legal reality may differ from social reality, if this discrepancy does not undermine regulatory objectives. They become an instrument of legal and economic efficiency, provided the link between form and substance does not become entirely arbitrary. This coherence between legal form and economic reality is essential for the legitimacy of these fictions. When this coherence fails - for example, when a company is used merely as a front for personal activities or to evade legal obligations - the veil lifting mechanism intervenes as a corrective response of the law.

In today's digital economy, where dominant entities often operate without a clear physical presence, transparent hierarchies, or accountability typical of traditional legal persons, these fictions begin to lose their legal power. We are at a moment when their critical revision becomes necessary. Without adaptation, the legal fictions risk becoming instruments for avoiding liability and mechanisms that disrupt normative balance, rather than facilitators of regulated economic activity.

Indeed, the emergence of digital platforms has introduced a new type of market entity, operating without visible physical infrastructure, without classic decision-making hierarchies, or a clearly defined number of employees. These aspects challenge the application of the traditional logic of legal personhood: when an algorithm decides, who is responsible? When the headquarters is virtual, where is the registered office? When users create value, who is the producer?

Digital platforms are business models that use online infrastructure to facilitate interactions, exchanges, or transactions between two or more distinct groups of users, often in real time⁵. Relevant examples include social networks (e.g., Facebook, Instagram), which connect users for content sharing and advertising; online marketplaces (e.g., Amazon, eBay), which link buyers and sellers of goods or services; and crowdsourcing platforms (e.g., Kickstarter, Upwork), which facilitate project funding or collaborative work.

Digital platforms commonly claim to act merely as technological intermediaries between users. However, numerous studies and investigations have shown that they, in reality, set rules, control flows, prioritize content, and influence behaviour. This form of "algorithmic governance" entails a high degree of operational control⁶. Platforms define access conditions, formulate pricing policies, select and exclude participants, apply automated sanctions, and collect massive amounts of user data. All these functions are far from neutral, reflecting economic and legal decisions that carry a certain level of responsibility.

Furthermore, the digital architecture of platforms - operating transnationally through networks of subsidiaries and opaque legal entities - allows for avoidance or fragmentation of legal norms. For instance, a platform may conduct economic activity in one state while being registered in another, with significant consequences for taxation and legal liability.

⁴ *Ibidem*

⁵ [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU\(2021\)656318_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf); Mouial-Bassilana et al. (2025, pp. 144–145).

⁶ For a detailed examination of algorithmic decision-making and oversight, see Kango (2025).

3. CJEU case law and the requalification of platforms

The Court of Justice of the European Union (CJEU) has been called upon several times to clarify the legal nature of digital platforms.

In Case C-434/15 – *Asociación Profesional Elite Taxi v. Uber Systems Spain*, the CJEU held that Uber does not merely provide an information society service, but organizes and manages a transport network, qualifying it as a transport service provider subject to specific regulations: (...) from the information available to the Court, it appears that Uber's intermediary service is based on the selection of non-professional drivers using their own vehicles, to whom the company provides an application without which, on the one hand, these drivers would not be in a position to provide transport services, and, on the other hand, individuals wishing to make an urban journey would not use their services. Furthermore, Uber exercises decisive influence over the conditions under which such drivers provide services. In particular, Uber, through its eponymous application, sets at least the maximum fare for each journey, charges this fare to the client before paying part of it to the non-professional driver, and exercises a degree of control over the quality of vehicles and drivers, as well as over driver behaviour, which may lead, if necessary, to their exclusion. Therefore, it must be considered that this intermediary service forms an integral part of an overall service whose main element is a transport service and thus does not qualify as an 'information society service' within the meaning of Article 1(2) of Directive 98/34, referred to in Article 2(a) of Directive 2000/31, but as a 'service in the field of transport' within the meaning of Article 2(2)(d) of Directive 2006/123 (paras. 39–40). Consequently, Uber cannot rely on the freedom to provide services under the E-Commerce Directive, since it does not merely provide an information society service, and it is subject to national transport regulations (paras. 42, 47).

In Case C-390/18 – *Airbnb Ireland v. AHTOP*, the Court reached a different conclusion, since Airbnb does not exercise the same degree of control over the content provided on its platform. The Court ruled that the services provided in this case qualify as information society services: (...) it must be answered to the first question that Article 2(a) of Directive 2000/31, referring to Article 1(1)(b) of Directive 2015/1535, is to be interpreted as meaning that an intermediary service whose purpose, through an electronic platform, is to connect, for a remuneration, potential tenants with professional or non-professional landlords offering short-term accommodation services, while providing a number of ancillary services, must be qualified as an 'information society service' falling within the scope of Directive 2000/31 (para. 69).

In Case C-692/19 – *B v. Yodel Delivery Network Ltd.*, the CJEU examined the legal classification of independent workers in the platform economy: having regard to all these factors, firstly, the independence of a courier, such as the one in the main proceedings, does not appear to be fictitious, and, secondly, there does not appear, a priori, to be a subordinate relationship between the courier and the alleged employer. In these circumstances, it is for the referring court to determine the professional status of B, taking into account all relevant factors concerning both the individual and the economic activity carried out, in accordance with Directive 2003/88 and the criteria established in the case law referred to in paragraphs 27–32 of this order (paras. 43–44). While the decision leaves room for interpretation, it acknowledges that apparent autonomy does not exclude a relationship of economic dependence that may justify legal protection.

In Cases C-148/21 and C-184/21, the Court held that: an operator of an online sales website which integrates, in addition to its own sales offers, an online marketplace, uses a sign identical to an EU trademark of another person for identical products, when third-party sellers offer such products on that marketplace without the consent of the trademark owner, if an informed and reasonably attentive normal user of the site establishes a connection between the services of the operator and the trademark. This is particularly relevant where, taking into account all relevant circumstances, the user may believe that the operator itself is selling the products in its own name and on its own account. Factors such as the operator presenting listings in a uniform manner, displaying its own logo on all offers, and providing additional services to third-party sellers, such as storage and shipping, are relevant in this respect (para. 54).

These rulings demonstrate a trend toward revealing the fiction of "neutral" intermediation and reclassifying the actual legal relationships in which platforms play an active role.

Indeed, until recently, digital platforms were treated under European and national regulations as "neutral" intermediaries, merely providing technological infrastructure to facilitate user interactions. Under this view, platforms bore limited responsibility for third-party content or products. This legal fiction assumed that

platforms should not be liable for users' actions, as their role was purely technical, without direct influence on the content sold or distributed. This approach allowed platforms to benefit from a favourable regime of limited liability under the E-Commerce Directive 2000/31/EC, which protects online intermediaries insofar as they are not actively involved in managing or modifying user-generated content⁷.

The requalification of digital platforms has profound legal and economic implications. Legally, online platforms are now treated more as active economic actors, required to comply with regulations on intellectual property and consumer protection. They no longer enjoy full immunity and must meet stricter obligations, including implementing measures to prevent counterfeiting and cooperating with trademark holders to remove illegal products⁸. Economically, reclassifying platforms as active market participants imposes new commercial responsibilities, as their regulatory treatment becomes more aligned with other economic entities directly involved in commerce. Platforms will face stricter oversight, while users will benefit from greater protection against fraud and counterfeiting⁹.

4. Toward a reconfiguration of platform responsibility

In the context of the algorithmic economy¹⁰, the need to reconceptualize the liability of legal entities becomes evident. The classical model — where corporate will is expressed through a collective body — becomes insufficient in the face of automated decision-making. This has led to new regulations and doctrinal ideas, which will be discussed in the following sections.

4.1 Digital Services Act (DSA)

In December 2020, the European Commission published the long-awaited proposal for a Digital Services Act (DSA), intended to update the regulatory framework for online platforms. The proposal is part of a broader legislative package that also includes the Digital Markets Act (DMA). Together, the DSA and DMA establish a new regulatory framework for digital services governance in the European Union. The DMA aims to ensure a competitive and fair digital market by setting ex-ante rules applicable only to large online platforms acting as “gatekeepers” between business users and end-users. In contrast, the DSA has a much broader scope and seeks to update existing rules regarding platform liability in providing digital services¹¹.

The DSA contributes three key elements to the regulatory framework for content moderation:

1. It establishes general liability rules for providers of intermediary services;
2. It introduces a regime of due diligence obligations, with special emphasis on online platforms, including social media;
3. It strengthens cooperation among national authorities responsible for enforcing online regulations.

Liability rules for online intermediary service providers, set out in Chapter II of the DSA, form the legal backdrop for content-related decisions made by platform operators and other digital intermediary service providers. These liability rules are complemented by multiple due diligence obligations for online intermediaries.

Since the new rules cover a wide range of intermediary services, the DSA does not apply a one-size-fits-all approach but follows a risk-based approach, establishing a catalogue of asymmetric due diligence obligations. This asymmetric regulatory model, where rules increase in number and strictness from Level 1 to Level 4, reflects the principle of proportionality:

⁷ For a discussion on platform neutrality, see Peguera (2022, pp. 681–684).

⁸ For an inquiry into the co-evolution of European digital law and platform technology, see Eckardt (2025, pp. 183–213).

⁹ EPRS_STU(2021)656318_EN.pdf; For a discussion on liability models applying to digital platforms, see Van Loo and Spier (2024).

¹⁰ See Egan (2025).

¹¹ <https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms>.

- Level 1: All online intermediary service providers must include information about their content moderation policy in their terms and conditions. They must also publish annual reports with clear and detailed information on moderation activities, including the use of automated tools.
- Level 2: Hosting service providers must establish harmonized notice-and-action mechanisms and justify content removal decisions with explicit reasoning.
- Level 3: Online platforms must offer users real opportunities to challenge content removal or labelling decisions, through both internal complaint mechanisms and external alternative dispute resolution systems.
- Level 4: Very large online platforms (VLOPs) and very large online search engines (VLOSEs) are subject to additional rules to ensure extensive public oversight of their content moderation practices.

The DSA emphasizes oversight and enforcement, dedicating a detailed chapter to implementation, cooperation, sanctions, and enforcement. Overall, the enforcement of due diligence obligations imposed by the DSA is shared between Member States and the European Commission.

4.2 Assigning legal personhood to autonomous digital entities

Assigning legal personhood to autonomous digital entities represents one of the most challenging frontiers in contemporary legal thought, questioning the anthropocentric structure of law itself. This idea requires a profound re-evaluation of the concept of “legal subject” and the fundamental criteria by which legal capacity is granted. Once digital entities - based on algorithms and self-governance - can participate in economic and social processes without direct human intervention, the legal system must decide whether, and how, such entities can become “legal actors”. This transition could mark not only an extension of the existing legal framework but a paradigm shift in how we conceptualize the relationship between technology, autonomy, and responsibility in law. With the rapid advancement of digital technologies - especially artificial intelligence (AI), machine learning, and decentralized blockchain architectures - new forms of autonomous action are emerging, capable of intervening in economic, social, and even legal processes without constant human supervision¹².

Autonomous digital entities are systems capable of independently pursuing their goals, interacting with their environment, and other systems without immediate human intervention¹³.

The major challenge lies in the fact that these entities lack will in the traditional sense, have no headquarters, no clearly delineated assets, and no legally recognized organs. Therefore, they cannot easily fit into the classical model of a legal person. Nevertheless, their social and economic impact is real: they can produce legal effects, generate harm, and interact with human users and clients.

This reality places increasing pressure on the legal system to answer a fundamental question: who is responsible for the actions of an autonomous digital entity?

In this respect, some proposals - such as the European Parliament’s 2017 report on civil law rules on robotics¹⁴ - suggest the possibility of a form of electronic legal personhood. This could allow digital entities to bear liability and be subject to legal obligations. However, this idea remains controversial, as it raises questions about the limits of juridical personification and the risks of creating “phantom legal actors” that cannot be effectively controlled¹⁵.

Therefore, the issue at stake is not merely technical but also ontological and normative: is the law ready to recognize non-human entities as autonomous legal subjects, and if so, under what conditions and with what safeguards?

¹² See for example For a discussion on the transition from artificial intelligence autonomy to legal personhood, see Ramirez (2023, pp. 1–16).

¹³ <https://www.sciencedirect.com/topics/computer-science/autonomous-agent>.

¹⁴ Report containing recommendations to the Commission on Civil Law Rules on Robotics | A8-0005/2017 | European Parliament; For an evaluation of electronic personhood and legal status in artificial intelligence, see Avila Negri (2021).

¹⁵ Avila Negri (2021); de Oliveira Ribeiro (2025).

4.3 Regulating “algorithmic accountability” through traceability, code audits, and decision transparency

With the accelerated development of artificial intelligence, the legal, ethical, and safety implications of its use are becoming increasingly relevant in both economic and social spheres. We are entering a new phase of the digital revolution, in which concepts such as legal liability, algorithmic fairness, bias reduction, and system security are no longer merely topics for interdisciplinary research but essential subjects on the public agenda, sitting at the intersection of engineering and social sciences¹⁶.

While the previous decade focused predominantly on “data protection,” attention has now shifted toward “algorithmic conduct.” In this new context, it is necessary to develop technologies, procedures, and standards capable of turning the phenomenon of “Big Algo” into an opportunity rather than a threat to governments, businesses, and society as a whole.

Algorithmic accountability regulation involves creating a legal framework that allows the identification and attribution of responsibility for decisions generated by automated systems¹⁷. Traceability entails the ability to reconstruct decision-making logic, data flows, and any human interventions that underpinned a decision made by an automated system. Practically, this means that every algorithmic decision must be retrospectively analysable to determine: what data was inputted into the system; what algorithmic model was used; what automated adjustments occurred; and whether any validation or human oversight mechanisms were applied¹⁸.

Algorithmic auditing is conceptualized as both a research activity and a practical process aimed at evaluating, monitoring, and ensuring the legality, ethics, and safety of algorithms, integrating socio-technical interventions to manage and supervise the risks associated with them. This practice encompasses emerging research areas such as algorithmic fairness, explainability, robustness, and privacy protection, as well as well-established themes such as data ethics, governance, and accountability. Similar to financial auditing, it is expected that in the future governments, companies, and society at large will request algorithmic audits - formal guarantees that the algorithms in use are legal, ethical, and safe¹⁹.

Algorithmic accountability also implies an obligation for entities developing and implementing algorithmic systems to inform users about: the existence of automated decision-making; the general criteria underlying these decisions; and the right to request explanations and contest outcomes.

Recent regulations, such as the Artificial Intelligence Act proposed by the European Commission and the Digital Services Act (DSA), already introduce concrete transparency requirements for certain operators, particularly high-risk system providers and very large online platforms. Transparency is important not only for individual user protection but also to ensure democratic and legitimate oversight of AI deployment in critical areas such as public administration, justice, healthcare, and education.

4.4 Establishing corporate governance obligations adapted to digital risks

The rapid development of digital technologies and the exponential growth of the data-driven economy have profoundly transformed the functioning of corporations, financial markets, and, more broadly, the architecture of the global economy. The emergence of artificial intelligence, algorithmic decision automation, interdependence with digital infrastructures, and cybersecurity vulnerabilities necessitate a substantial rethinking of corporate governance principles. In this context, adapting governance frameworks to digital risks

¹⁶ For framework models addressing algorithmic accountability, transparency, and risk management, see Blake (2024) and Koshiyama et al. (2024).

¹⁷ See also For a proposed unified framework addressing ethical and legal boundaries in artificial intelligence regulation, see Mansouri et al. (2025).

¹⁸ For a discussion on ethical implementation and frameworks for responsible algorithmic decision-making, see Breidbach (2024, Article 101031).

¹⁹ See Koshiyama et al. (2024).

is no longer optional but essential for protecting public interest, fundamental rights, and long-term corporate sustainability²⁰.

Effective digital governance begins with accountability at the highest decision-making level. Boards of directors and executive bodies must expand their traditional mandate to include active oversight of digital risks. This entails not only formal approval of IT policies but also a deep understanding of how algorithms and data influence organizational decisions. Monitoring AI usage, establishing ethical standards for data collection and utilization, preventing discriminatory algorithmic outcomes, and overseeing cybersecurity preparedness must become structural components of corporate governance²¹.

Algorithmic transparency is a core condition for accountability. Companies should be required to disclose, in a clear and accessible manner, how algorithmic systems influence strategic decisions, market behaviour, or results delivered to users. This obligation becomes critical where automated decisions have a direct impact on fundamental rights, for example, in recruitment, lending, differential pricing, content moderation, or access to essential services.

Algorithmic auditing is among the most promising emerging practices for controlling and evaluating digital risks. Similar to financial audits, algorithmic audits involve periodic and independent verification of automated systems used by a company. The objectives of these audits include identifying statistical biases, assessing the fairness of generated outcomes, verifying compliance with existing legislation (such as GDPR or anti-discrimination laws), and testing the robustness and safety of models. For algorithmic audits to be effective, a clear regulatory framework must exist, specifying audit frequency, authorized auditing entities, reporting formats, and the degree of transparency toward stakeholders.

In the long term, corporate governance adapted to digital risks must be supported by an institutional architecture that includes independent supervisory authorities, mandatory technical standards, legal liability mechanisms, and a specialized ecosystem of professionals in algorithmic auditing, digital ethics, and AI compliance.

5. CONCLUSION

In this paper, we aimed to examine the extent to which classical corporate law concepts - such as legal personhood, patrimonial autonomy, and limited liability - remain suitable in the era of digital platforms, and to identify the directions for reform emerging from European Union legislation and case law, as well as from doctrinal scholarship.

Indeed, the rise of digital platforms highlights the increasingly evident limits of legal fictions constructed during the industrial era, particularly the fictions of legal personhood and limited liability. Designed to encourage risk-taking in business and to separate the legal entity from its members, these fundamental instruments of corporate law functioned effectively in an economy based on tangible assets, hierarchical structures, and clearly defined commercial relationships. However, with the emergence of digital platforms - characterized by decentralized organization, algorithmic opacity, and an informal capacity to regulate markets and labour - these fictions are under unprecedented pressure.

In the new digital ecosystem, the legal form often masks a functional reality that is far more complex. Limited liability allows platforms to evade responsibility for the social and economic impact they generate, while simultaneously exerting *de facto* control over working conditions, market access, and the economic behaviour of third parties. This dissociation between form and function undermines the very rationale of legal protection and calls for a re-evaluation of how legal responsibility is assigned.

Corporate law, in turn, is challenged to go beyond its traditional formalism and to integrate new criteria of assessment: the structural power of the platform, the nature of the dependency relationships it creates, its

²⁰ https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/09/digitalisation-and-corporate-governance_287234ff/296d219f-en.pdf; For a regulatory perspective on AI-driven corporate governance, see Bello y Villarino and Bronitt (2024).

²¹ *Ibid.*

capacity for informal regulation, and its potential to generate systemic risks. Traditional legal fictions - useful in an industrial context - risk becoming obstacles to the efficient and equitable regulation of the digital economy.

Thus, the current challenge is not merely a technical adaptation of existing rules but a profound normative reconfiguration. If corporate law wishes to maintain its relevance in a platform-based economy, it must rethink its foundations: replacing form with substance, apparent neutrality with effective traceability, and treating algorithmic entities not merely as formal structures but as actors with real responsibility. Only in this way can coherence be ensured between the legal order and the emerging economic order—and only in this way can the balance between innovation, social justice, and the protection of the fundamental values of the rule of law be maintained.

REFERENCES

- Avila Negri, S. M. C. (2021). Robot as legal person: Electronic personhood in robotics and artificial intelligence. *Frontiers in Robotics and AI*, 8, Article 789327. <https://doi.org/10.3389/frobt.2021.789327>
- Barbière, J.-B. (2021). L'ordre sociétaire. LGDJ.
- Blake, H. (2024, October). Algorithmic accountability: Establishing frameworks for transparency and responsibility in AI-driven decisions. ResearchGate. https://www.researchgate.net/publication/387381860_Algorithmic_Accountability_Establishing_Frameworks_for_Transparency_and_Responsibility_in_AI-driven_Decisions
- Breidbach, C. F. (2024). Responsible algorithmic decision-making. *Organizational Dynamics*, 53(2), Article 101031. <https://doi.org/10.1016/j.orgdyn.2024.101031>
- de Oliveira Ribeiro, P. H. G. (2025). Socio-legal reflections on autonomous electronic agents as legal persons: Niklas Luhmann's sociology and digital personhood. In R. M. Becker et al. (Eds.), *Global perspectives on animism and autonomous technologies: Artificial intelligence, simulation and society* (pp. 145–165). Springer. https://doi.org/10.1007/978-3-031-88209-8_8
- Eckardt, M. (2025). EU digital law and the digital platform economy—an inquiry into the co-evolution of law and technology. *Review of Evolutionary Political Economy*, 6, 183–213. <https://doi.org/10.1007/s43253-024-00135-z>
- Egan, M. (2025). Towards a political economy of algorithmic capitalism. *Capital & Class*. Advance online publication. <https://doi.org/10.1177/03098168251326189>
- Gordon, J.-S. (2021). Artificial moral and legal personhood. *AI & SOCIETY*, 36, 457–471. <https://doi.org/10.1007/s00146-020-01063-2>
- Kango, U. (2025). Algorithmic governance. In W. Xu (Ed.), *Handbook of human-centered artificial intelligence*. Springer. https://doi.org/10.1007/978-981-97-8440-0_90-1
- Koshiyama, A., Kazim, E., & Treleaven, P. (2024). Towards algorithm auditing: Managing legal, ethical and technological risks of AI, ML and associated algorithms. *Royal Society Open Science*, 11(5), Article 230859. <https://doi.org/10.1098/rsos.230859>
- Mansouri, O., Yusuf, N., & Kooli, C. (2025). Ethical frontiers and legal boundaries: Proposing a unified framework for AI regulation and accountability. *Next Research*, 2(4), Article 101087.
- Mouial-Bassilana, E., Parachkevova, I., & Teller, M. (2025). *Droit des affaires en 12 thèmes: Avec exemples détaillés*. Dalloz.
- Peguera, M. (2022). The platform neutrality conundrum and the Digital Services Act. *IIC - International Review of Intellectual Property and Competition Law*, 53, 681–684. <https://doi.org/10.1007/s40319-022-01201-1>