IRASA International Scientific Conference
SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION
SETI VII 2025
Book of Proceedings
https://doi.org/10.62982/seti07.ivku.67

ALGORITHMIC GOVERNANCE AND ACCOUNTABILITY UNDER EU LAW

Ivica Kustura[309]

Abstract

The widespread embedding of algorithmic systems in economic sector has elicited a strong regulatory reaction from the European Union. This paper looks at the EU's evolving legal framework designed to harness algorithms and make them accountable, with particular attention paid to the landmark General Data Protection Regulation (GDPR), the proposed AI Act, the recently enacted Digital Services Act (DSA), and the Digital Markets Act (DMA). We also consider how these legislative pillars—ranging from the GDPR's foundational data protection principles and rights relating to automated decision-making, to the DSA/DMA's platform-specific transparency and risk management obligations, and the AI Act's horizontal risk-based approach—collectively strive to impose a comprehensive regime on algorithms. In reviewing these developments, we discerned several trends: towards risk-based regulation, for sure; but also towards making the invisible (the workings of algorithms) more open and apparent; and towards ensuring, in increasing numbers of cases, that a human being will be involved in any sufficiently consequential decision. Even as we note these trends, however, we have identified several emerging challenges that might impede the EU from realising the ambitious visions articulated in these landmark pieces of legislation.

Key words: *Algorithmic regulation, European Union law, General Data Protection Regulation (GDPR), Artificial Intelligence Act (AI Act), Digital Services Act (DSA), Digital Markets Act (DMA).*

Introduction

Algorithms have become an invisible yet decisive force in modern societies. They rank web search results, curate social media, assess welfare claims, suggest financial products, screen job applications, and even predict reoffending risks [1]. In doing so, they shape access to opportunities, resources, and rights. Once confined to narrow technical roles, algorithms now act as governance tools that sort, rank, and decide on matters touching justice and democracy [2].

[309] Ivica Kustura, MSc, Honorary Academician of IRASA, North University, Croatia, ikustura@unin.hr, ORCID 0000-0002-9974-6122

Their impact is both promising and troubling. Algorithms are celebrated for efficiency, scale, and objectivity: they process vast datasets, reveal hidden patterns, and bring consistency to decisions [3]. These strengths also have their dangers. Opaque design obscures accountability, biased data reproduces inequality, and private corporations often wield disproportionate informational power [4].

As a result, algorithms embody what sociologists call a "double-edged modernity": sources of empowerment but also domination [5]. The European Union (EU) has emerged as a global leader in regulating this landscape. Building on earlier data protection laws—most notably the GDPR—the EU has introduced a comprehensive framework: the Artificial Intelligence Act, which applies risk-based rules [6, 7], alongside the Digital Services Act and the Digital Markets Act, which demand transparency, accountability, and fair competition from platforms [8, 9]. Collectively, these are the most ambitious algorithmic regulations to date [10].

Through the "Brussels Effect," EU rules often set global norms, as multinational companies adapt to avoid costly non-compliance [11]. Just as the GDPR reshaped privacy standards, the AI Act, DSA, and DMA may establish worldwide models of accountability. This reflects the EU's aspiration to project its values—human dignity, democracy, and rule of law—beyond its borders [12]. But ambition does not guarantee success. Enforcement capacities vary across member states, risking fragmentation [13, 14]. Balancing rights with innovation remains contentious, and rivals pursue looser or more state-centric approaches [15]. The EU thus operates in a contested global arena where its leadership is both advanced and challenged [16].

This paper pursues four aims: to clarify the legal meaning of algorithmic accountability; to assess the GDPR, AI Act, DSA, and DMA, noting both strengths and limits; to identify emerging trends such as risk-based regulation, transparency as a binding duty, and mandatory human oversight; and to highlight challenges—weak enforcement, trade-offs with innovation, and normative gaps—that may constrain the EU's ambitions.

Literature review

Scholarly engagement with algorithmic governance has exploded in the past decade. Early work in law and political science framed algorithms as regulatory instruments in their own right. Yeung's influential analysis described algorithmic regulation as the substitution of rule-based law with data-driven systems that dynamically steer behaviour [2]. This perspective sparked debate about whether algorithms represent a form of "techno-regulation" or whether they can be assimilated into existing rule-of-law frameworks [17].

Legal scholars have examined the challenges algorithms pose to accountability. Binns argued that algorithmic systems often create "responsibility gaps," where harms cannot easily be traced to human actors [18]. Citron and Pasquale highlighted the danger of "black box" scoring systems in financial and employment contexts, warning of opaque and discriminatory decision-making [19]. Mittelstadt and colleagues systematised ethical concerns into six categories: epistemic opacity, fairness, responsibility, autonomy, trust, and power asymmetries [20].

Other research interrogates the limits of transparency. Ananny and Crawford [21] argued that transparency, while normatively attractive, often collapses under the complexity of socio-technical systems. Edwards and Veale [4] countered that meaningful disclosure obligations—such as those contained in the GDPR—can nonetheless create pathways for accountability. Wachter, Mittelstadt, and Floridi [3] went further, challenging the existence of a "right to explanation" in the GDPR, while conceding that explainability obligations may evolve in practice.

Philosophers and political theorists have developed the notion of digital constitutionalism: embedding fundamental rights and constitutional values into digital infrastructures [22]. Lynskey argues that data protection law provides a proto-constitutional framework but must evolve to address collective harms [23].

Empirical studies confirm that algorithmic systems reproduce structural inequalities. Buolamwini and Gebru's "Gender Shades" project demonstrated significant racial and gender bias in commercial facial recognition systems [65]. Barocas and Selbst [24] showed how "big data" analytics can generate disparate impacts, even absent intentional discrimination. Eubanks [25] documented the punitive effects of automated welfare systems on vulnerable populations, underscoring the need for algorithmic accountability.

Finally, policy scholarship identifies the EU as a global norm entrepreneur. The OECD's Principles on AI [26] and UNESCO's Recommendation on the Ethics of AI [27] explicitly echo EU values of transparency, fairness, and human rights. The Council of Europe's draft AI Convention [28] likewise reflects EU influence, positioning the region as the epicentre of algorithmic governance debates.

Taken together, this literature demonstrates that the EU's framework is both informed by and contributes to global academic, ethical, and policy discourses. However, tensions remain between transparency and opacity, individual and collective harms, and rights-based versus systemic approaches. These tensions frame the subsequent analysis of the GDPR, AI Act, and digital platform regulation [29, 30].

The GDPR as foundational pillar

The General Data Protection Regulation (GDPR) [6] represents the EU's most significant legal innovation in digital governance. Adopted in 2016 and enforced since May 2018, it provides a comprehensive framework for data protection that also directly addresses automated decision-making.

Rights against automated decision-making

Article 22 GDPR grants individuals the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them [6]. This provision acknowledges the profound impact of algorithmic decision-making on personal dignity and autonomy. Yet scholars like Edwards and Veale [4] argue that its scope is narrow, covering only decisions made entirely without human involvement. Hybrid

systems, where a nominal human oversight exists, may escape scrutiny—creating what they call a "loophole."

The GDPR permits automated decisions in limited cases—contract performance, explicit consent, or legal authorisation—but even then requires safeguards such as the right to human intervention, expression of views, and contestation [6]. This framework sets a global precedent for regulating automated decisions, though critics question its practical effectiveness.

Transparency and explainability

Articles 13–15 GDPR impose transparency obligations, requiring controllers to provide "meaningful information about the logic involved" in automated processing [6]. Wachter, Mittelstadt, and Floridi [3] argue that these provisions fall short of a true "right to explanation." Others, like Edwards and Veale [4], contend that when combined with accountability (Article 5), these duties could functionally evolve into explanation rights.

Enforcement practice demonstrates tension: the French CNIL stressed intelligible disclosure for laypersons [31], while the UK ICO emphasised the need to explain both purposes and consequences of processing. Scholars warn that disclosures risk devolving into "transparency theatre" [21], overwhelming individuals with technicalities or oversimplifications.

Accountability and DPIAs

The GDPR embeds accountability through Article 5(2), requiring controllers to demonstrate compliance. Article 35 mandates Data Protection Impact Assessments (DPIAs) when processing likely creates "high risks" to rights and freedoms. The Article 29 Working Party clarified that many algorithmic decision-making systems fall into this category [32].

Accountability thus shifts the compliance burden onto organisations, requiring proactive risk management rather than reactive enforcement.

Enforcement and jurisprudence

Enforcement has been mixed. Notable cases include:

- Schrems I (2015) [13]: CJEU invalidated the EU–US Safe Harbour agreement.
- Schrems II (2020) [14]: CJEU invalidated the Privacy Shield framework.
- SyRI Case (District Court of The Hague, 2020) [33]: Struck down algorithmic profiling in welfare as violating privacy rights.
- CNIL v. Google (2019) [34]: €50 million fine for transparency failures in personalised advertising.
- Spanish AEPD (2021) [35]: Sanctions for unlawful profiling in banking.
- UK ICO (2021) [36]: Scrutiny of algorithmic recruitment for potential bias.

These illustrate both the promise of GDPR and its enforcement challenges. While headline cases set strong precedents, many regulators lack the resources and expertise to audit complex AI systems.

Global influence

The GDPR's influence has spread worldwide. Brazil's LGPD (2018) [37], California's CCPA/CPRA [38], and China's PIPL (2021) [39] all incorporate GDPR-like protections, particularly concerning automated decisions. Scholars describe this as the "Brussels Effect" in practice [11].

Limitations

Despite its innovations, the GDPR faces critique:

- Narrow Article 22 scope [4].
- Limited transparency effectiveness [21].
- Unequal enforcement capacities across Member States [91].
- Focus on individual rather than collective harms [40].

Thus, while foundational, the GDPR is not sufficient alone—hence the need for the AI Act, DSA, and DMA.

The AI Act

Introduction: a landmark in algorithmic governance

The Artificial Intelligence Act (AI Act), proposed by the European Commission in April 2021 and adopted in June 2024 [7], marks the EU's most ambitious step in regulating AI directly. While the GDPR [6] addresses automated decision-making through the lens of data protection, the AI Act takes a technology-focused approach, creating a comprehensive risk-based framework. It reflects the EU's regulatory ambition to balance innovation with fundamental rights [41].

Risk-based classification

At the core of the AI Act is a **tiered risk-based classification system**:

1. Prohibited AI: AI practices deemed incompatible with EU values—such as manipulative subliminal techniques, exploitation of vulnerable groups, social scoring, and certain real-time biometric surveillance in public spaces—are outright banned [7].
2. High-risk AI: Annex III of the Act lists categories including biometric identification, critical infrastructure, education, employment, creditworthiness, migration, justice, and law enforcement.
3. Limited-risk AI: Transparency obligations apply (e.g., chatbots must disclose their artificial nature).
4. Minimal-risk AI: Most AI uses fall here, with no binding obligations beyond voluntary codes.

This risk framework draws on precedents in EU product safety law and the precautionary principle.

Obligations for high-risk systems

Providers of high-risk AI must comply with a set of stringent obligations:

- Risk management (Article 9).
- Training and testing data quality (Article 10).
- Technical documentation and record-keeping (Articles 11–12).
- Transparency obligations for users (Article 13).
- Human oversight (Article 14).
- Accuracy, robustness, and cybersecurity (Article 15).
- Conformity assessments and CE marking before placement on the market (Articles 16–43).

These obligations operationalise the accountability principle of the GDPR [6] into the AI domain.

Governance and enforcement

Enforcement is shared between national competent authorities and a new European Artificial Intelligence Board, with the Commission playing a coordinating role. A proposed EU AI Office will centralise expertise and oversee foundation models [42]. This multi-level structure aims to avoid the enforcement asymmetries observed under the GDPR.

Critiques of the AI Act

Scholars, NGOs, and industry stakeholders have raised concerns:

- Vagueness of definitions: The AI Act defines "AI" broadly, potentially sweeping in simple statistical systems [13].
- Compliance burdens for SMEs: High costs of conformity assessments risk creating market barriers [43].
- Scope limitations: Annex III excludes certain high-risk applications, such as predictive policing and emotion recognition, unless amended [44].
- Innovation paradox: Critics argue that strict rules may hinder EU competitiveness relative to the US and China [45].

Civil society calls for stronger prohibitions (especially against biometric surveillance) have clashed with industry demands for narrower obligations.

Global spillover

The AI Act's extraterritorial reach mirrors that of the GDPR [11]. Already, Canada's Artificial Intelligence and Data Act (AIDA) [46] and Brazil's draft AI Bill [47] draw heavily from its risk-based framework. Soft-law initiatives such as the OECD Principles [26] and UNESCO's Recommendation [27] also resonate with EU priorities. The US *Blueprint for an AI Bill of Rights* [48] indicates convergence on values (fairness, transparency, accountability) but lacks binding force. Meanwhile, China pursues a state-centric model, mandating algorithmic filing and content control [15].

Future outlook

The AI Act contentious issues include:

- Law enforcement exemptions for biometric surveillance [49].
- How to regulate general-purpose and foundation models [50].
- Capacity of regulators to supervise high-risk AI in practice.

The Act is likely to evolve dynamically, requiring amendments and delegated acts to remain future-proof.

The Digital Services Act and Digital Markets Act

Introduction: the digital services package

Alongside the GDPR [6] and AI Act [7], the Digital Services Act (DSA) [8] and Digital Markets Act (DMA) [9] form part of the EU's Digital Services Package, adopted in 2022. While the GDPR and AI Act target data protection and AI-specific risks, the DSA and DMA tackle structural issues of platform power—namely content moderation, disinformation, competition, and market fairness [51].

The Digital Services Act (DSA)

The DSA replaces the 2000 e-Commerce Directive (Directive 2000/31/EC) [52], updating liability and due diligence rules for online intermediaries.

Due diligence obligations

The DSA introduces obligations for all online intermediaries:

- Notice-and-action procedures for illegal content.
- Priority to "trusted flaggers" in moderation processes.
- Transparency reports on moderation, advertising, and recommender systems.

Very large online platforms (VLOPs)

Platforms with 45+ million users face additional obligations:

- Systemic risk assessments addressing disinformation, child protection, electoral integrity, and fundamental rights.
- Annual independent audits.
- Advertising transparency, including disclosure of sponsors and targeting criteria.
- Recommender system choice, offering non-profiling alternatives [8].

These provisions mark a shift from reactive liability to ex ante systemic accountability [10].

Enforcement

Oversight is two-tiered: national Digital Services Coordinators supervise smaller platforms, while the European Commission directly regulates VLOPs. Concerns remain about whether the Commission has sufficient staff and expertise.

The Digital Markets Act (DMA)

The DMA addresses competition imbalances in digital markets. It defines "gatekeepers" as platforms with entrenched intermediation power (e.g., search engines, app stores, marketplaces).

Core obligations

Gatekeepers must:

- Refrain from self-preferencing in rankings.
- Ensure interoperability of messaging services.
- Provide business users access to data generated through their activities.
- Obtain explicit consent before combining personal data across services.

These obligations echo remedies in EU competition law, such as *Google Search (Shopping)* (Case AT.39740) [53]. Unlike traditional antitrust enforcement, the DMA imposes ex ante rules to reduce lengthy litigation delays.

Sanctions

The Commission can impose fines of up to 10% of global turnover, rising to 20% for repeat infringements [9]. This deterrent mirrors the GDPR's penalty framework [6].

Complementarity of the DSA and DMA

While the DSA targets systemic rights and safety harms, the DMA addresses market fairness. Together, they expand algorithmic accountability from the level of individual rights (GDPR) and risk tiers (AI Act) to infrastructural regulation of platforms.

Critiques

Scholars and stakeholders highlight several challenges:

- Implementation capacity: Effective audits require expertise and resources beyond current institutional levels [54].
- Innovation concerns: Business groups warn obligations on interoperability and ad transparency may stifle EU competitiveness [55].
- Geopolitical tensions: The DMA disproportionately impacts US tech giants, provoking US trade complaints [56].
- Fundamental rights risks: NGOs warn that trusted flaggers and strict liability could incentivise over-removal of legitimate content [57].

Global influence

Like the GDPR, the DSA/DMA are expected to set global benchmarks [11]. Comparable initiatives include Japan's Act on Improving Transparency and Fairness of Digital Platforms (2021) [58], Australia's News Media Bargaining Code (2021) [59], and the US American Innovation and Choice Online Act (2021) [60].
China diverges, adopting a state-control model where platforms must file algorithms and promote "positive energy" content [15].

Remarks

The DSA and DMA represent a paradigm shift in platform regulation. They institutionalise systemic accountability, extending algorithmic governance from the realm of data and AI into market and information infrastructures. Their success, however, hinges on effective enforcement and international cooperation.

Challenges and tensions

Fragmented enforcement across member states

The GDPR [6] created a "one-stop shop" system where lead supervisory authorities handle cross-border cases. Yet disparities in expertise and resourcing among national authorities have led to uneven enforcement. Namely, Ireland's DPA, responsible for many major tech companies, has been criticised for delays [61].
Similar risks exist for the AI Act [7], where national competent authorities will enforce obligations. The DSA [8] attempts to avoid this by giving the European Commission direct oversight over VLOPs. Whether the Commission has the staff and expertise to fulfil this mandate is still debated [62].

Innovation versus regulation

The EU faces the innovation paradox: strict safeguards risk burdening SMEs while aiming to protect rights. Industry actors argue compliance costs under the AI Act and DMA [9] could stifle innovation [55]. Others argue regulation fosters innovation by providing trust and legal certainty [63]. This reflects a longstanding EU dilemma of balancing precaution with competitiveness.

Rights versus security

The EU struggles to balance fundamental rights and security imperatives. In AI Act negotiations, exceptions for law enforcement biometric surveillance remain highly contested [50]. Civil society groups warn these weaken rights protections [45].
The DSA's content moderation rules also raise concerns: automated filters for terrorist content may lead to over-removal and chilling effects on free expression [57]. Similar

tensions appeared in Digital Rights Ireland [30] and Schrems cases [13, 14], where security and privacy collided.

Global regulatory competition

The EU's model competes globally with US innovation-led and Chinese state-control frameworks. The US Trade Representative criticised the DMA as discriminatory [56]. China has framed EU regulation as a form of "digital imperialism" [64]. These disputes may fuel regulatory fragmentation, challenging global interoperability.

Individual versus collective harms

EU law historically emphasises individual rights (e.g., consent, transparency, contestation). Yet many algorithmic harms—disinformation, systemic bias, market concentration—are collective. The GDPR's individual focus [6] struggles with such issues. The DSA and DMA partly address collective dimensions, but doctrinal integration of collective accountability remains incomplete [65].

Technical and institutional capacity

Algorithmic audits require advanced expertise. Regulators often lack sufficient technical staff [29]. Independent audits mandated by the DSA [8] may risk becoming formalities unless supported by strong methodologies [66]. The EU's reliance on standardisation bodies like CEN-CENELEC for AI norms [67] is promising, but global harmonisation is slow.

Dynamic technologies and the "Pacing Problem"

The rise of foundation models challenges the AI Act's sector-specific design [50]. Legal frameworks often lag behind technology, a phenomenon dubbed the "pacing problem". Without adaptive governance tools, EU regulation risks obsolescence. [68] [69]

Conclusion

What the EU shows is that governing algorithms is not just a technical exercise but a constitutional one. Private tech firms now hold something close to public power, and the EU is trying to bind them with obligations usually reserved for States. By writing transparency, accountability, and human oversight directly into law, it has turned ideas of digital constitutionalism into enforceable duties.

This project also reflects Europe's identity as a "normative power." Through the so-called Brussels Effect, its rules shape practices well beyond its borders, especially when it comes to big tech.

The lesson, however, is that rules alone are not enough. Without serious enforcement, they risk becoming symbolic. And while precautionary rules are needed, they must also leave room for innovation. Looking ahead, Europe will have to keep updating.

The AI Act will evolve through delegated acts, the DSA may need stronger tools for systemic risks, and the DMA will likely tighten its gatekeeper rules.
None of this will matter without capacity and legitimacy across borders. The stakes go far beyond Europe. If this framework works, it could offer a model for balancing rights and innovation worldwide. If it does not work, the result may be fragmentation and a loss of democratic credibility. In the end, the way how Europe regulates algorithms may shape not only digital markets but democracy itself.

References

[1] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
[2] Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. https://doi.org/10.1111/rego.12158
[3] Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705.
[4] Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12. https://doi.org/10.1177/2053951715622512
[5] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs. https://doi.org/10.1007/s42438-019-00086-3
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, p. 1-144.
[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.
[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L 265, 12.10.2022, p. 1–66.
[10] Fasel, Mathieu. (2025). Is the Digital Services Act Here to Protect Users?: Platform Regulation and European Single Market Integration. Nordic Journal of European Law. 7. p. 72-95. https://doi.org/10.36969/njel.v7i4.27292.
[11] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
[12] Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, 1(6), 261–262. https://doi.org/10.1038/s42256-019-0055-y
[13] Case C-362/14, Maximillian Schrems v Data Protection Commissioner (Schrems I), ECLI:EU:C:2015:650.
[14] Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559.
[15] Creemers, R. (2025). The Regulation of Generative AI in China (22 Apr. 2025), in Philipp Hacker, and others (eds), *The Oxford Handbook of the Foundations and Regulation of Generative AI*, https://doi.org/10.1093/oxfordhb/9780198940272.013.0039.
[16] Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning*. MIT Press.

[17] Brownsword, R., & Goodwin, M. (2012). *Law and the technologies of the twenty-first century: Text and materials.* Cambridge: Cambridge University Press. https://doi.org/ https://doi.org/10.1017/CBO9781139047609
[18] Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (FAT)*, 149–159. https://doi.org/10.1145/3287560.3287592
[19] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33. Available at: https://digitalcommons.law.umaryland.edu/fac_pubs/1439 (accessed 18 September 2025).
[20] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. https://doi.org/10.1177/ 2053951716679679
[21] Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal. *New Media & Society*, 20(3), 973–989. https://doi.org/10.1177/1461444816676645
[22] Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(2), 76–99. https://doi.org/10.1080/13600869. 2019. 1562604
[23] Lynskey, O. (2019). Grappling with "data power": Normative nudges from data protection and privacy. *Theoretical Inquiries in Law*, 20(1), 189–220. https://doi.org/10.1515/til-2019-0007
[24] Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. https://doi.org/10.2139/ssrn.2477899
[25] Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. New York, NY: St. Martin's Press. ISBN: 9781250074317.
[26] OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Available at: https://oecd.ai/en/ai-principles (accessed 18 September 2025).
[27] UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. Adopted 24 November 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000380455 (accessed 18 August 2025).
[28] Council of Europe. (2022). Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Draft). Strasbourg: Council of Europe. Available at: https://www.coe.int/en/web/artificial-intelligence/ (accessed 18 September 2025).
[29] Binns, R. (2018). Algorithmic Accountability and Public Reason. *Philosophy & Technology*. 31. 1-14. https://doi.org/10.1007/s13347-017-0263-5.
[30] European Court of Justice (Grand Chamber). Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Judgment of 8 April 2014, ECLI:EU:C:2014:238. CURIA URL: https://curia.europa.eu/juris/liste.jsf?num=C-293/12 (accessed 18 September 2025).
[31] Commission Nationale de l'Informatique et des Libertés (CNIL). (2019). Délibération SAN-2019-001 of 21 January 2019 (Google LLC fine). Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 18 August 2025).
[32] Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA), WP248 rev.01. Brussels: European Commission. Available at: https://ec.europa.eu/newsroom/article29/items/611236 (accessed 18 August 2025).

[33] District Court of The Hague. (2020). NJCM c.s./De Staat der Nederlanden (SyRI), ECLI:NL:RBDHA:2020:187. English summary available at: https://pilpnjcm.nl/en/dossiers/syri (accessed 18 August 2025).
[34] CNIL. (2019). Google – sanction of €50 million. Press release, 21 January 2019. Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 18 August 2025).
[35] Agencia Española de Protección de Datos (AEPD). (2021). Sanction procedure PS/00477/2020. Madrid: AEPD. Available at: https://www.aepd.es/en/resolutions (accessed 18 August 2025).
[36] Information Commissioner's Office (ICO). (2021). Investigation into AI recruitment tools. London: ICO. Available at: https://ico.org.uk/about-the-ico/news-and-events/ai-recruitment-investigations (accessed 18 August 2025).
[37] Brazil. Law No. 13.709 of 14 August 2018, Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, 15 August 2018. English translation available at: https://lgpd-brazil.info/ (accessed 18 August 2025).
[38] State of California. (2018). California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq. Amended by the California Privacy Rights Act of 2020 (CPRA). Text available at: https://oag.ca.gov/privacy/ccpa (accessed 18 August 2025).
[39] National People's Congress of the People's Republic of China. (2021). Personal Information Protection Law (PIPL), adopted 20 August 2021, effective 1 November 2021. English translation available at: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021 (accessed 18 August 2025).
[40] Mittelstadt, B. (2017). From individual to group privacy in big data analytics. *Philosophy & Technology*, 30(4), 475–494. https://doi.org/10.1007/s13347-017-0253-7
[41] European Commission. (2019). The EU's approach to risk regulation in product safety. Brussels: Publications Office of the European Union. Available at: https://ec.europa.eu/growth/sectors/product-safety (accessed 18 August 2025).
[42] European Commission. (2023). Proposal for an EU AI Office. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/ai-office (accessed 18 August 2025).
[43] AlgorithmWatch. (2021). Position paper on the EU AI Act. Berlin: AlgorithmWatch. Available at: https://algorithmwatch.org/en/ai-act-position-paper (accessed 18 August 2025).
[44] European Parliamentary Research Service (EPRS). (2022). *The Artificial Intelligence Act: Strengths and weaknesses*. Brussels: European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)698839 (accessed 18 August 2025).
[45] Access Now. (2021). *EU AI Act: Civil society response*. Brussels: Access Now. Available at: https://www.accessnow.org/eu-ai-act-analysis (accessed 18 August 2025).
[46] Government of Canada. (2022). Artificial Intelligence and Data Act (Bill C-27). Ottawa: ISED. Available at: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act (accessed 18 August 2025).
[47] Brazilian Chamber of Deputies. (2022). Draft Artificial Intelligence Bill. Brasília: Câmara dos Deputados. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2318593 (accessed 17 September 2025).
[48] The White House. (2022). Blueprint for an AI Bill of Rights. Washington, DC: OSTP. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights (accessed 18 August 2025).

[49] Council of the European Union. (2023). Compromise text on the AI Act. Brussels: Council Secretariat. Available at: https://www.consilium.europa.eu/en/documents-publications (accessed 18 August 2025).
[50] Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S. & Liang, P. (2021). On the opportunities and risks of foundation models. *arXiv preprint*, arXiv:2108.07258. https://doi.org/10.48550/arXiv.2108.07258
[51] European Commission. (2020). Shaping Europe's digital future: Digital Services Package. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed 19 August 2025).
[52] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce (Directive on electronic commerce). Official Journal of the European Union, L 178, 17.7.2000, p. 1–16.
[53] European Commission. (2017). Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service (Case AT.39740). Brussels: European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784 (accessed 19 August 2025).
[54] European Court of Auditors. (2022). EU digital platform regulation: Challenges in oversight. Luxembourg: ECA. Available at: https://www.eca.europa.eu/en/publications (accessed 19 August 2025).
[55] BusinessEurope. (2022). Position paper on the DMA. Brussels: *BusinessEurope*. Available at: https://www.businesseurope.eu/publications/dma-position-paper (accessed 19 August 2025).
[56] Office of the United States Trade Representative (USTR). (2023). Report on foreign trade barriers – EU Digital Markets Act. Washington, DC: USTR. Available at: https://ustr.gov (accessed 19 August 2025).
[57] European Digital Rights (EDRi). (2021). Civil society analysis of the DSA. Brussels: *EDRi*. Available at: https://edri.org/our-work/civil-society-analysis-of-the-dsa (accessed 19 August 2025).
[58] Government of Japan. (2021). Act on Improving Transparency and Fairness of Digital Platforms. Tokyo: Ministry of Economy, Trade and Industry. Available at: https://www.meti.go.jp/english (accessed 19 August 2025).
[59] Australian Competition and Consumer Commission (ACCC). (2021). News Media and Digital Platforms Mandatory Bargaining Code. Canberra: ACCC. Available at: https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code (accessed 19 August 2025).
[60] United States Congress. (2021). American Innovation and Choice Online Act, S.2992, 117th Congress. Washington, DC: U.S. Government. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/2992 (accessed 19 August 2025).
[61] European Parliament. (2021). Report on the implementation of the General Data Protection Regulation two years after its application. 2020/2717(RSP). Strasbourg: European Parliament. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html (accessed 20 August 2025).
[62] European Commission. (2023). DSA enforcement capacity: Commission staffing plans. Brussels: European Commission. Available at: https://digital-strategy.ec.europa.eu/en/news/dsa-enforcement (accessed 20 August 2025).
[63] De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

[64] Ministry of Foreign Affairs of the People's Republic of China. (2022). Position paper on EU digital regulation. Beijing: *MFA*. Available at: https://www.fmprc.gov.cn (accessed 20 September 2025).
[65] Lynskey, Orla. (2019). Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*. 20. 189-220. https://doi.org/10.1515/til-2019-0007
[66] Algorithmic Auditing Research Network. (2022). Methodologies for auditing AI systems. Brussels: *AARN*. Available at: https://algorithmic-auditing.net (accessed 20 August 2025).
[67] CEN-CENELEC. (2021). Proposal for a Regulation laying down harmonized rules on artificial intelligence. Brussels: CEN-CENELEC. Available at: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/Position%20Paper/2021/positionpaper_aia_2021.pdf (accessed 20 September 2025).
[68] Hacker, P. (2022). AI Regulation in Europe: From the AI Act to Future Regulatory Challenges. *arXiv*. 14(2), 345–374. https://doi.org/10.48550/arXiv.2310.04072
[69] Marchant, G. E., Allenby, B. R., & Herkert, J. R. (2011). *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem*. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-1356-7