

Article

When Digitalization Meets Regulation across Borders: An Explainer with Actionable Insights

Eugenie Coche¹, Ans Kolk^{1a}

¹ University of Amsterdam, The Netherlands

Keywords: digitalization, regulation, data, privacy, digital strategy, platforms

<https://doi.org/10.46697/001c.122505>

AIB Insights

Vol. 24, Issue 3, 2024

A flurry of regulations has emerged across the world to govern the use, transfer and storage of data, affecting digital and traditional firms, of all sizes. To guide business practitioners and educators, this article provides insights into key components of digital laws and what they mean for different types of firms. We take the European Union as starting point, given its prominent and extra-territorial rule-setting, but also reflect on other cross-border (future) digital regulations. Our analysis of relevant details reveals a need for practitioners to be prepared and forward-looking, considering firms' specifics, internationally converging ethical principles and (future) digitally-aware generations.

INTRODUCTION

Recent years have seen an exponential rise in laws to govern the use, storage and transfer of data, affecting multinational enterprises (MNEs) in distinct ways (Coche, Kolk, & Ocelík, 2024). Despite regulatory convergences across countries and regions, variances – stemming from different traditions and motives – remain. While the European Union (EU) is often characterized by its strong focus on human rights, the United States on digital innovation and China on national security (Bradford, 2023), all jurisdictions share a growing urge for “technological sovereignty” (European Commission, 2020: 3). Accordingly, international business (IB) scholars are increasingly aware that “national context still matters in the digital age” (Meyer, Li, Brouthers, & Jean, 2023: 578). To guide practitioners and business educators, this article offers insights into key components of digital laws and what they mean for different types of MNEs. We take the EU as starting point given its prominent rule-setting on these topics, with the 2018 General Data Protection Regulation (GDPR) as well-known first case in point. The GDPR was introduced to strengthen Europeans' personal data protection rights. It broadened the definition of “personal data”; granted individuals new rights; imposed new obligations on firms; and gained global relevance through extra-territorial rules paired with fines (e.g., Meta's €1.2 billion fine). By regulating both EU and non-EU based firms, the GDPR played a pivotal role in MNEs' digitalization. More recently, the EU's digital strategy kicked in to regulate other aspects of digitalization (European Commission, 2020), primarily through five main acts complementing the GDPR (summarized in [Table 1](#)). Based on a le-

gal analysis and using the “Alphabet” firm as illustrative example (because of its market power and versatility), we uncover these act's distinct implications and identify three core insights relevant for IB and MNEs.

DIGITAL ACTS RELEVANT FOR IB

DIGITAL SERVICES ACT (DSA)

The DSA was created to make the online environment safer, namely to better counter illegal content, increase users' awareness of advertisement practices, tackle disinformation and clarify liability rules. It imposes due diligence obligations on all “online intermediaries”, including infrastructure and hosting service providers, online platforms and marketplaces. These obligations target hosted content (e.g., social media posts) and range from banning “dark patterns” (which e.g. make it hard for users to change their “by default” settings) to enabling users to notify and take down illegal content. Importantly, the act acknowledges firms' heterogeneity by taking into account size, impact and business model. Micro and small enterprises (i.e., less than 50 employees and annual turnover or balance sheet not exceeding €10 million) are exempted from numerous obligations (e.g., to provide yearly transparency reports) and hosting service providers (e.g., cloud services) face less rules than platforms (e.g., social networks) by being mainly required to have “notice-and-action” mechanisms in place. Amongst platforms, online marketplaces face additional obligations (e.g., to also collect information about their traders); while “very large online platform and search engines” (VLOPS) – designated as such by the EU Commission

^a Contact author: akolk@uva.nl

Table 1. Summary of EU Acts and implications for Alphabet

	Objectives	Extra-territorial application	Obligations reflect firms'			Concrete implications for Alphabet	
			Business model		Size	Legal obligations include	Practical actions include
DSA	Tackle illegal content online	Applies irrespective of a firm's place of establishment (Art 2(1))	Only applies to online intermediaries	Less obligations for hosting service providers Amongst platforms, more obligations for marketplaces	-Less obligations for micro and small enterprises -More obligations for VLOPS	Youtube (VLOPS): -Increased transparency towards users - Content moderation tools - Annual systemic risks assessments	Youtube blocked targeted ads for minors & rolled out a new transparency center
DMA	Fair competition	Ibid. (Art 1(2))	Only applies to gatekeepers offering core platform services	Obligations vary between types of platforms (e.g., app stores; search engines)	Gatekeeper threshold only covers very large firms	Google Search cannot list its Google Shopping services more favorably than those of competitors	Google introduced dedicated "aggregator units" and "refinement chips" in its Google Search services (easier for users to compare results)
DA	Enhance access to IoT and public sector data	Ibid. (Art 1(3))	Different obligations for IoT manufacturers or data processing service providers (including cloud & edge services)		Gatekeepers should not receive data; micro-and small enterprises should not share data	Google smartwatch data must, by default, be easily accessible to its users and, upon request, to non-Google market players	Google introduced its "home APIs" (i.e., Application Programming Interface) to enable data sharing from smart home devices
DGA	Enhance trust in data-sharing	Ibid. (Art 11(3) jo. 19(3))	Different obligations for data altruism and data intermediation firms		N.A.	Notify competent EU authority about future data intermediation service and set up a separate legal entity	N.A (at the moment, Alphabet does not offer such services)
AIA	Ensure trustworthiness and fairness of AI systems	Ibid. (Art 2(1))	-Different obligations for AI providers, deployers, importers and distributors -Certain AI-driven business models (e.g., social scoring systems; general-purpose AI models) are prohibited or regulated in specific ways		Favored treatment for micro and small enterprises	Gemini must make its users aware that they interact with an AI system and all technical information about its AI model must be kept up to date	Google joined the Coalition for Content Provenance and Authenticity to foster transparency in AI-generated content

based on their number of active users (i.e., more than 45 million) – are subject to the strictest regime.

As VLOP, Alphabet has obligations for YouTube, including the need to conduct yearly “systemic risks” assessments to counter pre-defined risks (e.g., unfair electoral processes) and apply adequate mitigation measures (e.g., adapting algorithms).

DIGITAL MARKETS ACT (DMA)

Complementing the DSA, the DMA primarily addresses market imbalances to ensure that the digital market is as contestable and open as possible. To understand its *raison d’être*, a mere reference to the Google Shopping case (Persch, 2021), which started in 2010 but is still debated, suffices: the search engine was found to put its own services on top, relegating competitors, but the EU could only intervene after damage had occurred. The DMA aims to help the EU prevent anticompetitive behaviors. It therefore imposes obligations and restrictions on “gatekeepers” – dominant platforms able to twist digital markets in their favor. Six firms – all foreign-based and including Alphabet – met the act’s cumulative threshold when adopted, being important in the EU in terms of annual turnover (at least €7.5 billion) and acting as gateways for business (i.e., 45 million monthly active EU users and 10,000 yearly active EU-based business users in the three last financial years). Firms designated as such must proactively refrain from engaging in unfair practices. This includes a ban to combine users’ personal data across distinct platforms, to self-preference own services or to “lock-in” users.

Google Android is, for instance, not allowed anymore to force its users to choose Google Chrome as default search engine or Google Play as app store. Likewise, the DMA introduces obligations to enable users to access and share data, closely intertwined with the data strategy explained below.

DATA ACT (DA)

The EU’s data strategy – subpart of its digital strategy – aims to optimize the value of data across all economic sectors. It complements earlier data liberalization initiatives such as the GDPR’s data portability right (i.e., for individuals to access data about them) and sector-specific laws requiring firms to share data with third parties (e.g., open banking). Amongst its novelties, the DA introduces data-sharing obligations in relation to Internet of Things (IoT) data (i.e., emanating from connected devices). It establishes business-to-consumer, business-to-business and business-to-government data-sharing rules, while accounting for firm heterogeneity (e.g., gatekeepers should not receive data; micro and small enterprises should not share data). A key obligation for IoT manufacturers is to design and manufacture their connected products in such a way that users and third parties can “by default” (i.e., without user intervention) and free of charge access generated data.

Hence, Alphabet needs to ensure its Google smartwatch data can easily be accessed by, for example, non-Google (repair) services. The act further compels firms to share data in

a “fair, reasonable and non-discriminatory” manner, with restrictions on compensation costs (e.g., clearly based on firms’ costs to collect, produce and make the requested data available), and in using such data for developing competing products. For example, data recipients cannot use Google smartwatch data to create a smartwatch of their own.

DATA GOVERNANCE ACT (DGA)

Complementing the DA, the DGA aims to make data more accessible and foster data-driven innovation. Unlike the DA, which concerns mandatory data-sharing situations, the DGA seeks to facilitate and build trust for voluntary data-sharing practices. It includes rules to encourage the growth of two types of services: “data altruism” organizations and “data intermediaries”. The first category enables individuals and companies to share their data for altruistic ends, such as fighting pollution. These organizations can be registered as trusted if they are not-for-profit and meet certain requirements of the EU’s “rulebook” (e.g., data must be stored securely). In contrast, data intermediation services are for-profit firms supposed to act as neutral third parties in data-sharing transactions (e.g., data marketplaces such as the French Dawex). Because of significant market powers of platform-based businesses, the DGA requires these firms (potentially Alphabet in case it would develop such services) to notify competent EU authorities. They also need to meet obligations such as fair use of data (e.g., data cannot be used for other reasons than data disposal), unbundling of data services (in a separate legal entity) and fair and non-discriminatory pricing.

ARTIFICIAL INTELLIGENCE ACT (AIA)

The AIA regulates the use of AI systems, which refer to any machine-based system that allows firms to generate “outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”. To make these systems trustworthy, the act imposes obligations and restrictions on all actors involved in the AI value chain: AI providers (i.e., developers of systems), deployers (i.e., users of systems), importers and distributors. Crucially, as part of the EU’s risk-based approach, all actors have to examine the purpose of the AI system and, in turn, assess its risks, which can be unacceptable; high; limited; or minimal. The first category entails an exhaustive list of AI practices (e.g., social-scoring systems) that are prohibited. The second concerns AI systems involving major societal risks, such as automated hiring or credit-scoring systems, which the act allows in case all its far-reaching obligations are met. This includes the need for AI providers to do pre-market “conformity assessments” (following technical, legal and ethical requirements) prior to putting their services on the EU market, and AI deployers to perform “fundamental rights impact assessments” (including identification of specific risks and human oversight measures). The third category is seen as less risky (e.g., chatbots, deepfake generators, general-purpose AI (GPAI) models) for which the act mainly requires transparency towards users and downstream system providers, with ad-

ditional obligations for GPAI models presenting “systemic risks” (i.e., having high impact capabilities, taking computer power of training models into account). Finally, the AIA subjects minimal-risk AI systems, such as spam filters or AI-enabled video games, to voluntary codes of conduct.

Hence, in case Alphabet’s Gemini service (meant as ChatGPT ‘competitor’) classifies as a systemic risk GPAI model, its obligations include the need to assess and mitigate such risks, perform model evaluations and implement adequate cybersecurity measures.

TOWARDS ACTIONABLE INSIGHTS

The five acts discussed above have direct relevance for EU firms, *and* for MNEs based in other, non-EU countries, as the Alphabet example illustrates. Crucially, these regulations cover a range of data-related issues reflecting developments across the world. Interestingly, although the EU has no “domestic” big tech gatekeeper firms, its digital rule-setting stretches beyond the region. This extraterritoriality also applies to some EU regulation in other domains such as sustainability (see examples in [Table 2](#)). While a so-called “Brussels effect” (Bradford, 2019), whereby the EU influences regulatory and corporate changes outside of its borders through its regulatory first moves, can be seen as negative (burdensome) or positive (value-based governance), we posit that restrictions on digitalization are simply a reality to be coped with – with more to come, also in other countries (cf. [Table 2](#)). Moreover, with “gen Z” and “gen Alfa” as students and (future) employees, digital awareness is becoming widespread. To be prepared, practitioners and business educators may use three insights from our legal analysis.

First, the Brussels effect, which was obvious already with the GDPR (Bradford, 2019; Coche, Kolk, & Ocelík, 2024), will likely extend to the acts discussed in our article, most notably the AIA (Siegmann & Anderljung, 2022). Importantly, since these acts are “regulations” (not “directives”), they instantly become part of Member States’ national laws, thus having an EU-wide application straightaway. As such, for firms with activities in the EU, this provides clarity and may facilitate their growth, not just within but also outside the EU. This also means that foreign-based MNEs might benefit from being forward-looking and implementing emerging EU rules immediately, to be prepared if other countries adopt them in some form in the (near) future ([Table 2](#)). Doing so could create a competitive advantage vis-à-vis (global) trading partners or prevent a disadvantage, especially when consumers are increasingly aware of their data privacy rights. Hence, leaving the EU market – as “X” suggested in relation to the DSA – may not be the most appropriate response in view of future regulatory trends worldwide.

Second, since these laws affect all MNEs and not merely digital-only firms (cf. Stallkamp, 2021), we recommend all practitioners to make data governance a priority, considering their firms’ specifics. This could involve front-end design (e.g., more transparency towards users) and back-end system changes (e.g., data-sharing technologies); as

well as business model and/or value chains reconfigurations (e.g., responsible AI contractors). However, as illustrated by Meta’s “pay or okay” business model shift (i.e., users either pay or consent to behavioral advertising) – controversial under the GDPR (EDPB, 2024), the DMA and the DSA – firms should approach these laws holistically (i.e., considering all relevant dimensions). In view of the AIA, this also means for MNEs to adopt a risk-based approach towards all their digital activities and, hence, to assess these in light of human rights and internationally converging ethical principles (e.g., “fairness”; “trustworthiness”; OECD, 2024). Besides helping MNEs save (future) litigation and reputation costs, doing so might also help meet “privacy-conscious” shareholders’ interests (SEC, 2023: proposal 15).

Third, to favor such ethically-driven firm behavior, we recommend that business educators make their students (i.e., future practitioners, also users of digital services) fully aware of the human rights implications of data-driven and AI-powered technologies. At the very least, this requires leaving behind the idea that firms “own” customer data, which is legally invalid but still suggested in the IB literature (cf., Madan, Savani, & Katsikeas, 2022). Indeed, data’s non-rivalrous nature, paired with its infinite value potential (i.e., big data) and human rights entanglements (e.g., data privacy), makes it an ambiguous object of property (cf. Geiregat, 2022). This explains the rise of new governance models, as well as MNEs’ growing data-sharing obligations (Coche, Kolk, & Dekker, 2024: 19).

CONCLUSIONS

This article took the EU as starting point to show how IB is affected by regulation. We discussed five acts that shape digitalization of MNEs not just within but also outside the EU, and used the Alphabet case to illustrate how these laws complement one another and influence the activities of a foreign-based big tech gatekeeper firm (cf. [Table 1](#)). Our exposition of the EU digital regulatory landscape, with attention for the specifics of each law, shifts away from the broad strokes often adopted in IB studies. These laws’ influential and potential Brussels effect contrasts with assumptions that it is rather exceptional for nations to “coordinate their legal frameworks internationally through for example the WTO or the EU” (Meyer et al., 2023: 582). Likewise, when merely taking a helicopter view of these acts, MNE managers or IB educators may associate them with (new) “techno-nationalism” (Luo & Van Assche, 2023) or geo-political measures. However, the EU acts primarily embody an ambition to ensure that technologies – irrespective of firms’ countries of origin – are fully aligned with European values (Irion, Burri, Kolk, & Milan, 2021). Whilst the resulting regulatory package may particularly affect foreign-based firms, this is due to their market power and peculiarities, not their nationality. Although we realize that views on the pros and cons of the EU approach may differ widely, our article aimed to provide somewhat deeper insights, also by including examples of other cross-border (future) regulations that include extraterritoriality, put forward by other countries around the world ([Table 2](#)). Prac-

Table 2. Examples of (future) extraterritorial rule-setting, within and beyond the EU

	(Proposed) laws	Extra-territorial scope	Similarities with EU digital laws
Non-EU digital laws/policies	UK's Digital Markets, Competition and Consumers Act (2022)	Also applies to non-UK firms (i.e., digital activity linked to the UK)	Imposes precautionary obligations on "strategic market status" firms (resembling the DMA in relation to gatekeepers)
	US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023)	Imposes reporting obligations on foreign resellers of US infrastructure-as-a-service-providers (e.g., cloud), in relation to the training of large AI models	Although a mere guidance (i.e., not a law) for privately-owned companies (unlike the AIA), it shows a commitment to a risk and principle-based approach to AI regulation (eight principles, including respect for privacy and civil rights)
	Canada's proposed Artificial Intelligence and Data Act (2022)	Also applies to international trade in AI systems	Risk-based assessment and classification of AI systems (resembling the AIA)
	Brazil's proposed AI Regulation (2023)	Also applies to foreign firms developing/implementing/using AI systems in Brazil	Ibid.
	Australia's Consumer Data Right Rules (2020)	Also applies to consumer data generated/collected outside Australia	Imposes data-sharing obligations in different sectors, starting with banking (broadly aligns with the DA as it may apply to IoT data in the future)
	Brazil's proposed law on Freedom, Responsibility and Transparency in the Internet (2020)	Also applies to foreign firms offering social media, search engines and instant messaging services to Brazilian citizens	Imposes transparency and accountability obligations towards hosted content (resembling the DSA)
EU laws on sustainability	Corporate Sustainability Reporting Directive (2022)	Also imposes reporting obligations on non-EU companies	Risk-based approach to firms' digital activities, as it imposes transparency obligations in relation to human rights risks (including data privacy)
	Corporate Sustainability Due Diligence Directive (2024)	Also imposes assessment and risk mitigation obligations on non-EU companies	Ibid., as it imposes due diligence obligations in relation to human rights risks (including data privacy) in firms' value chains

tioners and business educators may profit from our explainer, also in their interactions with digitally-aware generations interested in the societal and ethical aspects of digitalization.

ACKNOWLEDGMENTS

We would like to thank the three anonymous reviewers for their insightful and in-depth comments on our original and revised paper, and the editor for his support.

ABOUT THE AUTHORS

Eugénie Coche is a doctoral candidate at the Amsterdam Business School, University of Amsterdam, the Netherlands. Having a background in information law, her research interests lie at the intersection between law and international business, with a particular focus on the busi-

ness and societal implications of digitalization policies. Central to her current project, funded by ABN AMRO, is exploring the tension between data privacy, security and innovation, as well as finding out how multinationals navigate associated cross-border challenges.

Ans Kolk is Full Professor at the University of Amsterdam, Amsterdam Business School, the Netherlands. Her areas of expertise are in corporate social responsibility, sustainable development, and sustainability, especially in relation to international firms and their interactions with regulators and other stakeholders. One stream of research, on which she has published extensively in business and interdisciplinary outlets, involves the societal, ethical and environmental implications of novel data-based technologies and digitalization strategies. For more information, see <http://www.anskolk.eu/>

Submitted: March 17, 2024 EDT, Accepted: August 13, 2024 EDT



This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CCBY-4.0). View this license's legal deed at <http://creativecommons.org/licenses/by/4.0> and legal code at <http://creativecommons.org/licenses/by/4.0/legalcode> for more information.

REFERENCES

- Bradford, A. 2019. *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Bradford, A. 2023. *Digital empires: The global battle to regulate technology*. Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>.
- Coche, E., Kolk, A., & Dekker, M. 2024. Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector. *Internet Policy Review*, 13(1): 1–32.
- Coche, E., Kolk, A., & Ocelík, V. 2024. Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, 7: 112–127.
- EDPB. 2024. *Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms*. Brussels.
- European Commission. 2020. *Shaping Europe's digital future*. Luxembourg: Publication office of the European Union.
- Geiregat, S. 2022. *Who owns 'your' (business's) digital data? New EU law in the making*. <https://blogs.law.ox.ac.uk/oblb/blog-post/2022/12/who-owns-your-business-digital-data-new-eu-law-making>.
- Irion, K., Burri, M., Kolk, A., & Milan, S. 2021. Governing “European values” inside data flows: Interdisciplinary perspectives. *Internet Policy Review*, 10(3): 1–14.
- Luo, Y., & Van Assche, A. 2023. The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act. *Journal of International Business Studies*, 54: 1432–1440.
- Madan, S., Savani, K., & Katsikeas, C. S. 2022. Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, 54: 731–754.
- Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R.-J. “Bryan.” 2023. International business in the digital age: Global strategies in a world of national institutions. *Journal of International Business Studies*, 54: 577–598.
- OECD. 2024. *Recommendation of the Council on artificial intelligence*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.
- Persh, J. 2021. *Google Shopping: The general court takes its position*. <https://competitionlawblog.kluwercompetitionlaw.com/2021/11/15/google-shopping-the-general-court-takes-its-position/>.
- SEC. 2023. *Notice of 2023 annual meeting of stockholders and proxy statement*. California: United States Securities and Exchange Commission.
- Siegmann, C., & Anderljung, M. 2022. *The Brussels effect and artificial intelligence: How EU regulation will impact the global AI market*. Centre for the Governance of AI. https://cdn.governance.ai/Brussels_Effect_GovAI.pdf.
- Stallkamp, M. 2021. After Tik Tok: International Business and the Splinternet. *AIB Insights*, 21(2). <https://doi.org/10.46697/001c.21943>.