LUISS

Institute for European
Analysis and Policy

Hub for New Industrial Policy
& Economic Governance

Digital Industrial Policy: What are the future challenges?

Maria Savona and Filippo Bontadini

LUHNIP Working Paper Series 3/2025

February 12, 2025

Digital Industrial Policy:
What are the future challenges?

Maria Savona[1] & Filippo Bontadini[2]

Executive Summary

The digital transition is based on the emergence of digital automation technologies, including, but not limited to, Artificial Intelligence (AI). Most of the emerging digital technologies are based on the use of large amount of data, including, but not limited to, personal data of consumers and workers. This raises issues of asymmetries between individual consumers and workers, as personal data subjects, and the public and private actors (large tech, platforms, public administrations and governments that acquire and manage data for different purposes). These asymmetries are – for instance - related to value distribution, information, exposure to harmful effect of technologies, countries geopolitical relationships. To effectively address the governance of emerging digital automation technologies and data, a multidisciplinary approach is crucial. This requires expertise spanning across technical, legal, geopolitical, and economic fields. This working paper highlights some areas where these asymmetries remain relatively under-researched and insufficiently addressed by current European Union (EU) digital regulations, including the recent AI Act. One such area is data sharing, where further research is needed to explore governance mechanisms for both individual and business-to-business (B2B) data sharing. This could involve either mandatory rules or the creation of incentives that encourage sharing. Another area of concern is the uneven geographic distribution of digital infrastructure. A further area is the EU digital regulatory framework. Here we consider whether the AI Act will trigger a new wave of what has been termed the "Brussels effect," which refers to the EU's ability to influence global regulatory standards. While the EU's approach is commendable, there remains room for improvement, further research, and greater public scrutiny to ensure that the regulations are both effective and equitable. Ultimately, the goal is not to propose specific policy instruments, but to highlight the potential risks associated with failing to design appropriate tools for digital industrial policy.

[1] Luiss Institute for European Analysis and Policy, DEF, Luiss University, Rome & Science Policy Research Unit, University of Sussex, UK, msavona@luiss.it

[2] Luiss Institute for European Analysis and Policy, DIM, Luiss University, Rome & Science Policy Research Unit, University of Sussex, UK, fbontadini@luiss.it

1. Introduction

This working paper aims to offer insights on the importance of placing data governance at the centre of the 'digital industrial policy' agenda, that is, the rationale and the instruments specifically focused on the digital transition. The digital transition raises novel challenges – compared to previous waves of technological transformations - that require awareness of the specific side effects of leaving these challenges unaddressed.

The digital transition is based on the emergence of digital automation technologies, including, but not limited to, Artificial Intelligence. Digital automation technologies require both physical investments in digital infrastructures such as data centres and cloud storages and intangible investments in data base and software. Most of the emerging digital technologies (see Savona et al., 2021 for a taxonomy of these digital technologies) are in fact based on the use of large amounts of data, including, but not limited to, personal data on consumers and workers.

This raises issues of *asymmetries* between individual consumers and workers, as personal data subjects, and the public and private actors (large tech, platforms, public administrations and governments) that acquire and manage data for different purposes. There are also *asymmetries* in the geographical distribution of digital infrastructures across countries.

It is important to set a policy agenda for a digital industrial policy that puts at its centre the governance of data with the aim of reducing such asymmetries between different actors at different levels of analysis involved in the governance of data acquisition and management. It is not only a matter of data extractivism (Rikap, 2023), nor only a matter of individual privacy protection (Goos and Savona, 2024). We offer here some brief reflections on what we consider the future relevant challenges that would benefit from more policy-relevant research.

There are fundamentally two reasons why we believe the issues addressed here are under-researched:

First, the unprecedented pace of development of digital automation technologies and artificial intelligence (AI) makes the identification of such effects and the formulation of tools for addressing challenges very complex.

Second, addressing the governance of emerging digital automation technologies and data requires a true multidisciplinary perspective, including techno-legal, political and economic expertise.

The *techno-legal* perspective concerns the pervasiveness of AI applications and the need to regulate them in very diverse realms, which are often at odds with each other (e. g., the attribution of intellectual property rights on AI-generated art; the protection of privacy in increasingly complex data-treating business models).

The *geopolitical* perspective, specific to AI, seems to have sparked a wave of "new protectionism" and ensuing tensions among China, the US and the EU on basically every aspect related to digitalization, from domestic chipmaking to the regulation of digital trade and cross-border data flows "with trust" (OECD 2022).

The *economic* perspective includes, for instance, the need to adapt and possibly "upgrade" competition and antitrust regulations to digital markets; mitigate the effects of digital automation on labour markets; ensure a fair and inclusive redistribution of both the private and social value generated by (personal and business) data among firms, individual data subjects and public actors.

Here we focus on two examples that have been selected as they are relatively under-researched, would require a strong multidisciplinary effort and, most importantly, are clear examples of the asymmetries mentioned above:

- Data Sharing: Research on governing the process of data sharing at the individual and institutional levels, either through mandatory rules or the creation of incentives for sharing.
- Digital Infrastructures: there seem to be an uneven geography of the concentration of digital infrastructure, with countries with more stringent data protection, IP or tax regimes offshoring cloud services and data hubs to countries with weaker ones.

Finally, we acknowledge that the EU has been at the forefront of providing an articulated regulatory framework for steering the digital transition, as it has been historically for previous waves of Information and Communication Technologies. Within this context, it is relevant to evaluate whether the AI Act might be able to compensate for the effects of the asymmetries mentioned above, even though it may require further debate and public scrutiny on such effects and might lead to a new wave of the so-called "Brussels effect".

2. Data sharing

The economic nature of data changes along the data "value chain," which includes the aggregation, processing and analytics of individual data[3] (Corrado et al. 2022; Goos and Savona 2024). Individual data is a *club good*, excludable but not rivalrous (Savona 2019), as individuals or businesses might prevent the use of their personal or copyright-protected[4] information. However, once shared, data can be re-used at virtually no marginal costs. A legally owned database is a *private good*, excludable, and rivalrous, and is usually included in the intangible assets of firms (Corrado et al. 2022), being thus a source of comparative advantage. The ensuing data analytics is

[3] Personal data means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (article 4(1), EU GDPR, 2018).

[4] EU Directive 96/9/EC of 11 March 1996 recognizes the legal ownership of databases to firms, with *database property rights* being a legal category implemented in that context.

valuable information that eventually becomes collective knowledge whose economic nature is inherently a public good.

Depending on the actors involved and the purpose that information and collective knowledge serve, data presents the challenge of having to reconcile objectives that are often at odds with each other. For instance, it is important to create incentives to *maximise data sharing* for purposes of public interest such as health, mobility, or research. However, data as an asset in firms that benefit from inherent network economies requires *capping private value concentration* from an antitrust perspective. Facilitating data sharing and preventing value concentration might be at odds with *protecting individual privacy and other rights* (Savona 2020 and 2021; Goos and Savona 2024).

The European Commission has been trying to resolve this policy conundrum in the context of the articulated regulatory framework developed over the past few years and considered a benchmark worldwide (see Zenner et al., 2024, for updated data on the EU regulations in the digital sector over the past decade).

An interesting instance of such EU regulations is the EU Data Governance Act (DGA), which has explicitly aimed to foster the "*availability of data for use by increasing trust in data intermediaries and by strengthening data sharing mechanisms across the EU*". The focus is on the creation of data markets by legitimizing data intermediaries (i.e., data trusts, cooperatives, stewards, unions). Furthermore, it aims to "*make public sector data available for re-use (…) on altruistic grounds*".

Data intermediaries are supposed to act in the interests of individual data subjects and facilitate data sharing (Savona 2021; Goos and Savona 2024). However, to achieve a sufficient scale of aggregate information that serves public purposes such as research and public health, data intermediaries would need large-scale digital infrastructure to manage large amounts of data, which might lead to the same challenges that current big techs pose, such as market concentration, privacy leakages, and cybersecurity.

In addition, trustees that operate on a fiduciary basis on behalf of a group of individual data subjects should demonstrate a commitment to pro-social and "altruistic" behaviour, supported by appropriate incentives. This is not trivial.

A governance model that enforces data sharing for public interest has been proposed for the design and launch of the green mobility plan of the City State of Hamburg (The New Institute 2023). Within the legal framework designed in this case, data sharing has been made mandatory, rather than delegated to voluntary data trusts. The characteristics of the data sharing legal and technical framework for the green mobility plan in Hamburg have been described,

presented,[5] and discussed, although the outcome and the effectiveness have yet to be assessed, as the implementation is on-going.

[5] A New Digital Industrial Policy and Data Governance for the Public Interest. LUISS LEAP, 27 October 2023.

Similarly, the effectiveness of the DGA in creating missing data markets through data intermediaries is yet to be assessed, but it would be important that the intermediaries be capped in scale, limited to specific purposes, and monitored by an independent governing body to minimize the risks of shifting from big tech to big trusts.

Gräef and Prufer (2021) propose a governance framework for B2B data sharing that aims at avoiding market concentration. From a legal perspective, they claim that data sharing should be made mandatory and regulated and propose three potential models.

The first model would be a fully centralized one, involving a central role for a European Data Sharing Agency that would manage mandatory data sharing. The second model would be fully decentralized, involving the creation of a Data Sharing Cooperation Board, which would oversee a network of National Competition Authorities (NCAs) whose remit would be to enforce data-sharing contracts. The third one would be a hybrid model, with both centralized and decentralized features.

Governing the process of individual and B2B data sharing, either through mandatory rules or the creation and maintenance of incentives for sharing that do not lower consumer and citizens' protection, is no easy task. Overall, research and case studies on the creation and implementation of regulatory frameworks with different degrees of centralization are still in their infancy, let alone the assessment of their effectiveness. This is likely to become a crucial research and policy agenda in the near future.

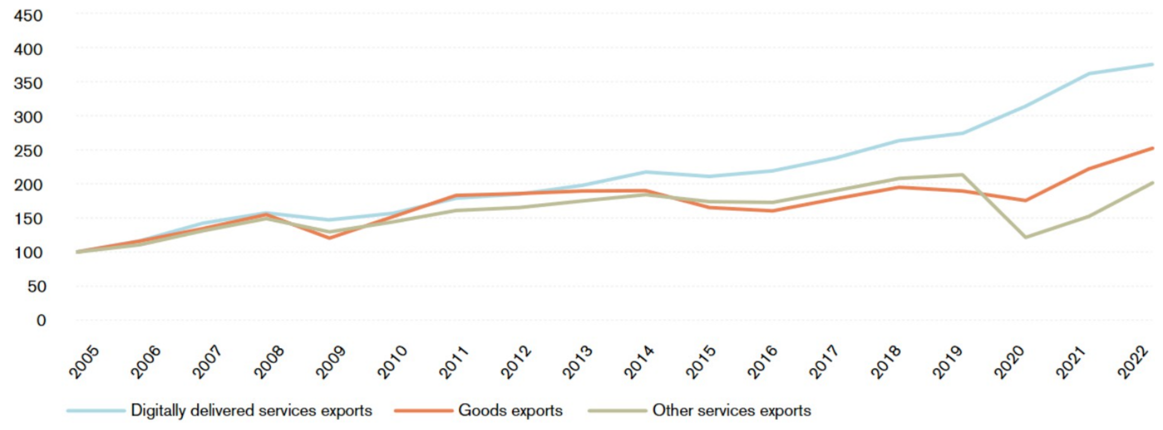
3. The geopolitics of digital infrastructure

Trade in digital services has increased considerably over the past decades (Figure 1) and relies on the investment capacity in physical digital infrastructure that supports cross-border data flows, including submarine cables, optic fibres, and, more recently, data centres and cloud storage of data and software. Data centres and cloud service providers are the tangible

component of investments in emerging digital technologies such as data acquisition, data management, software, artificial intelligence, which are intangible in nature (Savona et al., 2022; Corrado et al., 2023).

As firms increasingly invest in emerging digital technologies, they need to scale up their capacity to process large data in a cost-effective and reliable manner. According to the IMF, the OECD, the UN, the WTO (2023), *"Cloud computing services, defined as "computing, data storage, software, and related IT services accessed remotely over a network, supplied on demand and with measured resource usage that allows charging on a pay-per-use basis* ***are increasingly used to replace ownership of on-premises IT equipment****."*

Figure 1: Growth of goods, services and digitally delivered services exports (2005=100)



Source: WTO (2023).

Source: WTO (2023) as reported in Papadakis and Savona (2024)

This means that particularly when the scale of digital activity increases, the costs of storing and processing data lead companies to outsource (and offshore) data stocks and data management services to external cloud service providers and data centres.

Papadakis and Savona (2024) look at the geographical distribution of data centres and cloud service providers. Trends of digital service trade emerge as not the only factor underpinning the concentration of digital infrastructure in certain countries: Papadakis and Savona (2024) find that, not unexpectedly, high shares of global data centres are located in the US, Germany, and the UK, which are also the top digital services exporting countries. However, interestingly, the intensity (number of data centres per GDP or population) of data centres and cloud services is higher in a few small countries,[6] most of which are tax havens,[7] and are not necessarily specialised in digital services nor are the top digital services exporters. In addition, the uneven geography of data centres is relevant in the context of what we consider the new geopolitics of digital infrastructure, which we spell out as a 'data haven hypothesis' (Papadakis and Savona, 2024). We attempt a preliminary interpretation below.

First, the concentration of digital infrastructure might mirror the asymmetrical distribution of (digital) trade among headquarters and factory countries (Baldwin and López-González 2015), with large core countries offshoring digital infrastructure to peripheral and small economies, reproducing a core-periphery structure of digital trade.

Second, a high concentration of digital infrastructure in specific countries might be due to regulatory arbitrage, including the articulated EU digital regulations mentioned in the previous

[6] Gibraltar, Isle of Man, Jersey, Liechtenstein, Bermuda, Guernsey are among the countries with the highest intensity in data hubs per million capita (Papadakis and Savona, 2024).

[7] The Tax Justice Network assigns a Haven Score (HS) which measures the extent that a country's tax jurisdiction and financial system allow for corporations' tax abuse. The HS takes values from 0 to 100. The countries that rank at the top (≥85 HS) according to the HS are British Virgin Islands, Cayman Islands, Bermuda, Switzerland, Jersey, Singapore, United Arab Emirates, Bahamas, Cyprus, Guernsey, Isle of Man, Turks and Caicos Islands, and Anguilla.

section, the EU adequacy regulations on digital trade (see e.g., Ferracane et al. 2023; Bacchus et al. 2024), and intellectual property (IP) regulatory regimes (Santancreu 2023). Data hubs and might be concentrated in countries that are destinations of IP profit shifting or patent boxes[8] (Haufler and Schindler 2023; Alstadsæter et al. 2018; Accoto et al. 2023).

Third, in Papadakis and Savona (2024) we put forward the concept of a 'data-haven hypothesis' and argue that this might explain the asymmetries in the concentration of digital infrastructure, similarly to how the "pollution-haven hypothesis" has explained patterns of trade of green and brown products. We conjecture that – similarly to how advanced countries offshore activities that would not meet their strict environmental regulations to mid- and low-income countries with less stringent regulations (see Savona and Ciarli 2020 for a selected review) - countries with more stringent data protection, or IP or tax regimes regulatory frameworks, would offshore cloud services and data hubs to countries with more favourable tax regimes, for instance to benefit from favourable tax-rates on IP related profits, or laxer data protection regulations. There are contributions that have looked at the role of patent boxes[7] (Alstadsæter et al., 2018; Accoto et al., 2023).

The idea of increasing 'data governance interoperability' (Bacchus et al. 2024), which suggests making national digital regulations interoperable across countries, might go in the direction of strengthening the role of national governments vis-à-vis private owners of data centres or cloud services. The plea for international cooperation to ensure interoperability of data governance regimes should be extended beyond data protection to other realms, including IP and tax regulation.

4. The EU AI Act

The European regulatory framework of digital technologies has always been at the forefront of what has been named the "Brussels effect": when the General Data Protection Regulation became law, US tech giants had to comply, and several governments chose to align themselves with the main principles and rules to protect citizens' privacy – and digital rights – more broadly.

After a long gestation time, the most recent addition to the EU digital regulations (Zenner et al., 2024) is the EU Artificial Intelligence Act, which aims to regulate broad applications of AI in the Union to prevent potential harmful effects of 'high risk' AI applications. The initial paragraph of the Act effectively summarises the context and principles of the regulation.[9]

[8] Patent boxes are used to incentivise businesses to invest in R&D by taxing patent revenues at lower tax rates than other business revenues.

[9] "The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of

From the perspective of a digital law expert, Edwards (2022) identifies the boundaries of the AI Act, which, she claims, *"needs to be read in the context of other major packages such as the Digital Service Act (DSA), the Digital Market Act (DMA) and the Digital Governance Act (DGA)."* The first two primarily regulate large commercial platforms and the private sector, while the DGA is concerned with data intermediaries and incentives to individual and institutional data sharing (see discussion above).

The AI Act, instead, is mainly, though not solely, aimed at the regulation of AI systems' use in the public sector. In addition, its scope covers the applications (albeit those of course emerged up to now) that carry the risk of harmful effects, from "high risk", such as biometric recognition, predictive policing, social scoring, deepfake, and algorithmic management in workplaces, to "minimal risk" such as the private sector targeted marketing.

The EU AI Act includes not only a systematization of high-risk cases, but also the objective of regulating foundation models such as Large Language Models, which have sparked much debate in the case of generative AI. As has been pointed out, the regulation of foundation models is at the root of AI governance, and this is essentially what will be at stake over the next few years. Notably, obligations to comply fall mainly on providers, though also on importers and distributors too.

It has been pointed out (Edwards, 2021; Veale and Borgesius, 2021) that the Act's aim is rightly ambitious, yet it might be too broad in its scope. Despite the ambition, it seems that it fails to provide general criteria for AI risk assessment. The lack of general criteria might make the Act unfit to be applied to the future numerous applications that are still untapped. In addition, the focus on the 'providers' compliance to risk minimization might fail to trace the responsibility of other downstream actors, and certainly end users, who seem to have no role and no agency in the regulatory framework of the AI Act.

As already mentioned, it would be important to be aware of the development of the technology, the complexification of the actors involved in the creation, adoption and use of AI in firms and the public sector, and the specificities of sectoral applications. There is obviously a high degree of uncertainty in both the future development of the technology and in the future degree of pervasiveness in different sectors. This is the main reason why it is important to define general, foundational criteria of risk assessment, which countries preparing for complying with the Act can receive.

As is well known, the US hosts the largest number of giant digital platforms. It will be interesting to see whether the EU Artificial Intelligence Act will trigger another Brussels

effect. It would be important to monitor the effects of compliance, and the effect of the lack of or weak compliance in areas that are crucial in view of the (still uncertain) development and

Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation." (EU AI Act, 2024).

diffusion of Artificial Intelligence's applications.

This opens a Pandora's box and leads to the second point: under the Biden administration, there have been hints of the US moving closer to the EU's regulatory framework (Ruiz and Savona, 2023). One of the issues at stake is the alleged copyright infringement on digital texts copied from the web and used to train LLMs and generative AI. It is well known how the debate has been nurtured by the cases of the *New York Times* and, separately, eight others American newspapers owned by Alden Global Capital – including the *Chicago Tribune* and *New York Daily News* – suing OpenAI and Microsoft. In the *New York Times* instance, the complaint crucially goes beyond the infringement of copyright law and lays down the case for regulating AI more broadly, borrowing much of the thrust and the principles of risk-adverse and rights preservation contained in the EU AI Act. It raises concerns that touch upon misinformation, the protection of human creativity, the social value of professional and truthful journalism, as well as democracy itself. A highly reputable US company is suing a formerly non-profit and now for-profit billion-heavy US company.

A further instance where the US has moved quite unexpectedly toward the EU regulatory framework is in the sudden change of its position on digital trade (Ruiz and Savona 2024). In October 2023 the US announced that it was withdrawing its position on digital trade from the WTO to allow for stronger regulation. This might certainly be in line with the protectionism strategy in the context of geopolitical tensions mentioned above and the US' desire to maintain its supremacy in the global AI race. However, it is not inconsistent with the Biden administration's Blueprint for the AI Bill of Rights.

In sum, the EU AI Act is a tremendous effort to prevent potential harmful effects that might result from the lack of governance of AI applications. Still, the technology itself has yet to develop its full potential, and the uncertainties linked to an increase of the still limited use of AI in new sectors are still high. The Act may require further debate and public scrutiny in the near future.

5. Conclusions and Policy recommendations

This paper has focused on the future challenges of the governance of emerging digital technologies, with Artificial Intelligence being among them. We consider them of high policy relevance but they are relatively under-researched. While we do not aim to provide specific policy instruments, we rather aim to raise the potential side effects of failing to design appropriate digital industrial policy tools to tackle the issues mentioned here. There is a lot of untapped potential for the development of these technologies and hence their governance.

As briefly argued above, one of the challenges of AI and data governance is to reconcile often conflicting objectives: to create (and maintain) incentives to maximize data sharing for purposes of public interest, such as health or research; to limit the concentration of private value arising from (involuntary or voluntary) data collection and analytics as in the case of LLM training; to protect privacy and other individual rights such as copyright in a context where human creativity (still) has social value.

In terms of data sharing, it would be important to combine elements of *mandatory regulations*, particularly when it comes to B2B exchanges in contexts that are of public interest, with the identification and implementation of the *right incentives to share data* for 'altruistic' purposes. We are not fully convinced that personal data intermediaries or a series of sectoral data trusts are the solution, as we have argued elsewhere (Savona, 2021).

In terms of digital infrastructures, mapping their global presence would be an important starting point. The research (and policy relevance) on this topic is still in its infancy. The normative implications of a high concentration of digital infrastructures will depend on a careful assessment of the environmental impact and geopolitical implications for hosting countries.

All this requires thinking out of the box and relying on a multidisciplinary understanding of (i) what the (economic) detrimental effects of a badly or non-regulated technology are, linked with (ii) carefully designed legal frameworks that prevent or internalize these externalities, alongside a (iii) forward-looking view of how the geopolitics of technology and the striking asymmetries in the lobbying powers of different actors involved play out.

References

Accoto, N., Federico, S., & Oddo, G. (2023). Trade in services related to intangibles and the profit shifting hypothesis *Temi di discussione* (Economic working papers) 1414, Bank of Italy, Economic Research and International Relations Area.

Alstadsæter, A., Barrios, S., Nicodeme, G., Skonieczna, A. M., & Vezzani, A. (2018). Patent boxes design, patents location, and local R&D *Economic Policy*, 33(93), 131–177.

Bacchus, J., Borchert, I., Morita-Jaeger, M., & Ruiz Macpherson, J. (2024). Interoperability of data governance regimes: Challenges for digital trade policy *CITP Briefing Paper* (No. 12, 2024).

Baldwin, R., & López-González, J. (2015). Supply-chain trade: A portrait of global patterns and several testable hypotheses *The World Economy*, 38(11), 1682-1721.

Corrado, C., Haskel, J., Iommi, M., Jona-Lasinio, C., & Bontadini, F. (2022). Data, intangible capital and productivity In Technology, productivity and economic growth *National Bureau of Economic Research* https://www.nber.org/books-and-chapters/technology-productivity-and-economic-growth/data-intangible-capital-and-productivity.

Edwards, L. (2022). The EU AI Act: A summary of its significance and scope *Ada Lovelace Institute* https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf.

European Commission (2022). *European Data Governance Act*: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission (2023). *Data Act* https://digital-strategy.ec.europa.eu/en/policies/data-act

European Commission (2024). *Artificial Intelligence Act* EU Artificial Intelligence Act.

Ferracane, M., Hoekman, B., van der Marel, E., & Santi, F. (2023). Digital trade, data protection and EU adequacy decisions *CIP Working Paper* (No 6, October 2023).

Goos, M., & Savona, M. (2024). The governance of artificial intelligence: Harnessing opportunities and mitigating challenges *Research Policy*, 53(3), 104928.

Graef, I., & Prüfer, J. (2021). Governance of data sharing: A law & economics proposal *Research Policy*, 50(9).

Haufler, A., & Schindler, D. (2023). Attracting profit shifting or fostering innovation? On patent boxes and R&D subsidies *European Economic Review*, 155.

IMF, OECD, UN, WTO (2023). *Handbook on Measuring Digital Trade* (2nd ed.).

Papadakis, I. and Savona, M. (2024). *The Uneven Geography of Digital Infrastructure. Does it Matter?* Luiss Institute for European Analysis and Policy, Policy Brief 14/2024, October 2024.

Rikap, C. (2023). Intellectual monopolies as a new pattern of innovation and technological regime *Industrial and Corporate Change*, 33(5), 1037–1062.

Ruiz, J., & Savona, M. (2023). The US turn is reshaping the geopolitics of digital trade What does this mean for the UK? *CITP Blog* (December 2023).

Santacreu, A. M. (2023). International technology licensing, intellectual property rights and tax havens *The Review of Economics and Statistics.*

Savona, M., & Ciarli, T. (2019). Structural changes and sustainability: A selected review of the empirical evidence *Ecological Economics*, 159, 244-260.

Savona, M. (2019). The value of data: Towards a framework to redistribute it *SPRU Working Paper Series* (SWPS), 2019-21, 1-22 https://www.sussex.ac.uk/spru/swps2019-21

Savona, M. (2020). Governance models for redistribution of data value *VOX CEPR* https://voxeu.org/article/governance-models-redistribution-data-value.

Savona, M. (2021). Dati, serve più chiarezza sugli intermediary che piacciono all'Unione *Il Sole 24 Ore*, 5th May 2021.

The New Institute New Hanse Blueprint (2023). Governing urban data for the public interest *Hamburg* (October 2023).

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act *Computer Law Review International*, 22(4), 97-112.

Zenner, K., Scott, M., & Sekut, J. (2024). A dataset on EU legislation for the digital world *Bruegel Factsheet* https://www.bruegel.org/system/files/2024-06/Bruegel_factsheet_2024_0.pdf