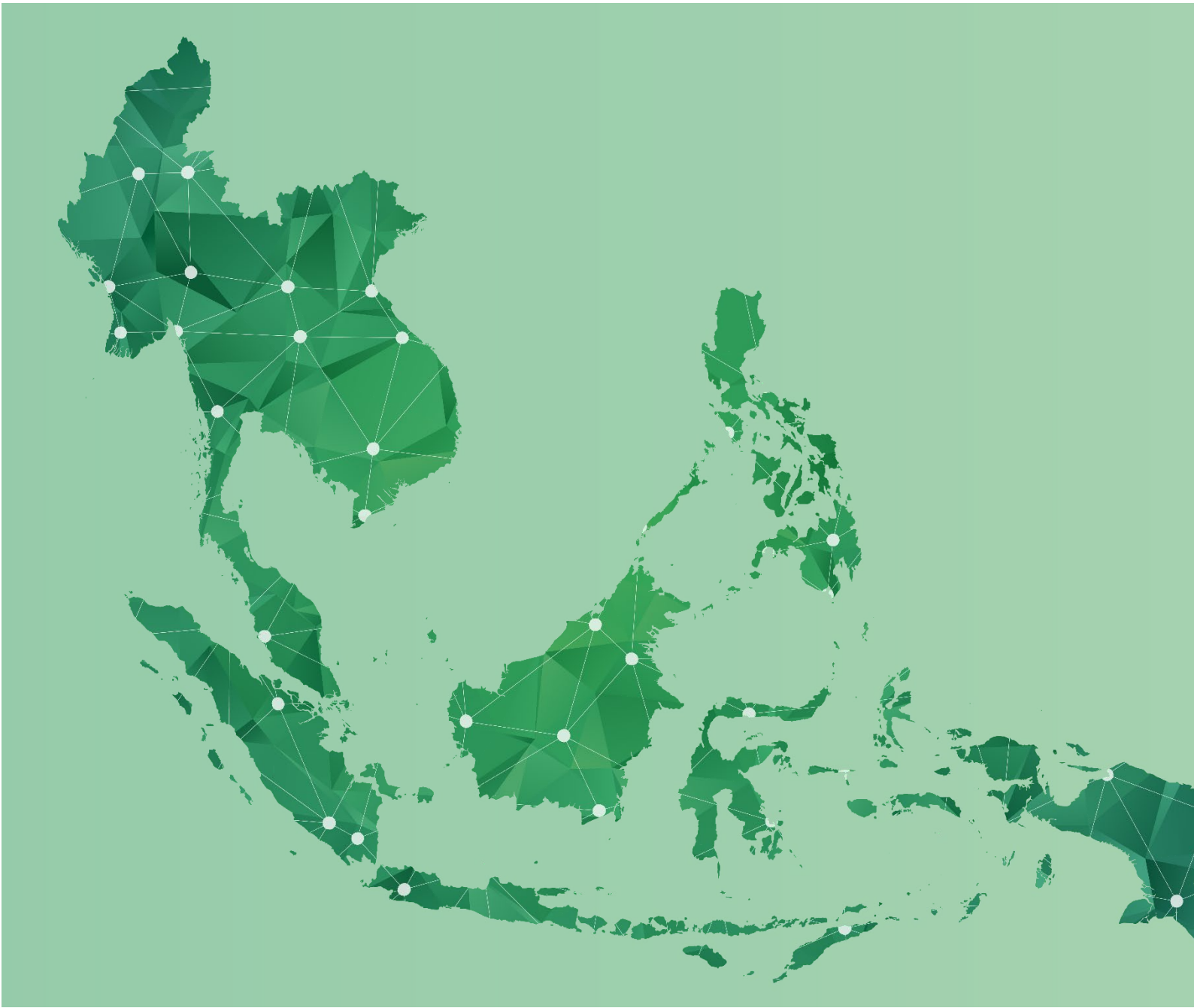
UNIVERSITY OF CAMBRIDGE | Cambridge Industrial Innovation Policy | IfM Engage | LR Foundation | UNIDO

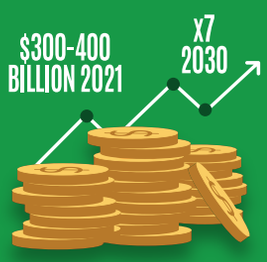
Rising risks and digital trade policy in Southeast Asia

A POLICY BRIEF DRAWING ON DATA FROM THE LLOYD'S REGISTER FOUNDATION WORLD RISK POLL

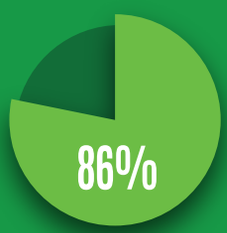


How can digital trade policies promote both innovation and public trust?

Digital trade is a growing part of everyday life, from sharing data, to using cloud services, and buying online. It brings convenience and opportunity, but trust can be undermined by cyberattacks and data misuse.



Southeast Asia's digital economy is expanding rapidly
Valued at $300–400 billion in 2021, ASEAN's digital economy could grow sevenfold under the ASEAN Digital Economy Framework Agreement (DEFA).

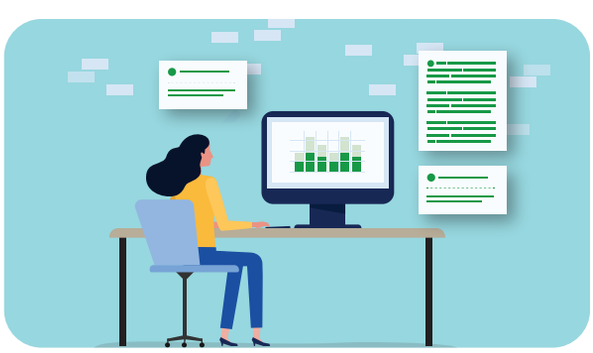


Trust at risk
86% of people in Southeast Asia are concerned about their data being stolen.

Countries balance openness with data security
Countries perceiving higher digital risks retain more policy space, avoiding commitments on free data flows or localisation bans.

ASEAN is fast progressing towards digital regulation
However, there is divergence in terms of data governance, cybersecurity, and e-commerce regulation.

POLICY RECOMMENDATIONS



1. Embed a risk-based approach in digital trade agreements
This includes creating flexible, tiered provisions for data governance and AI regulation that reflect national capacities.

2. Foster regional cooperation on AI standards and capacity building
This can include shared technical standards, resource-sharing platforms, and capacity-building programmes to align governance frameworks over time.

3. Strengthen the ASEAN Guide on AI Governance and Ethics with actionable tools
Examples include monitoring frameworks, auditing guidelines, and country-level roadmaps.

4. Promote inclusive dialogue and collaboration on new technologies to ensure policies keep pace
Digital policy forums can foster trust and reduce the risk of cross-border legal disputes through informed cooperation.

POLICY RECOMMENDATIONS

About this policy brief

This policy brief draws on the World Risk Poll (WRP) to examine recent trends in data privacy and data security and how digital trade governance is addressing these things. Insights from the WRP are integrated with data from UNCTADstat, the OECD's Digital Services Trade Restrictiveness Index (DSTRI), and the Trade Agreement Provisions on Electronic-commerce and Data (TAPED) data set. The policy brief provides policy recommendations for Southeast Asian countries, and beyond, on how digital trade governance can reduce data privacy and data security risks.

The brief forms part of a broader series, "Policymaking for a more resilient world: Leveraging the World Risk Poll for more effective digital, labour, and industrial policies", funded by Lloyd's Register Foundation, which aims to translate public perception data into actionable policy recommendations.

Contributors

Authors: Karishma Banga, Department of Digital Humanities, King's College London

Deep Mehta, Institute of Development Studies

Stakeholder engagement: Yulisyah Putri Daulay

Contents

List of abbreviations

AfCFTA	African Continental Free Trade Agreement
AI	Artificial intelligence
ASEAN	Association of Southeast Asian Nations
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEA	Digital economy agreement
DEFA	Digital Economy Framework Agreement
DEPA	Digital Economy Partnership Agreement
DSTRI	Digital Services Trade Restrictiveness Index
DTA	Digital trade agreement
ICT	Information and communication technology
MSME	Micro, small and medium enterprises
OECD	Organisation for Economic Co-operation and Development
PTA	Preferential Trade Agreement
RCEP	Regional Comprehensive Economic Partnership
USMCA	United States–Mexico–Canada Agreement
WTO	World Trade Organization

Executive summary

This policy brief draws on data from the Lloyd's Register Foundation World Risk Poll (WRP) to explore public perceptions of digital risk – particularly those related to data privacy and artificial intelligence (AI) – and how these concerns influence digital trade policy. It is part of a broader series focused on evidence-based policy options aimed at reducing risk and improving health and safety outcomes across Southeast Asia, supported by Lloyd's Register Foundation.

As digital technologies and digital trade become more widespread, concerns about their socio-economic effects have also increased. In response, this brief seeks to:

a) understand the core challenges facing digital trade in the ASEAN region
b) analyse how perceptions of digital risk shape digital trade policy
c) analyse the fragmented landscape of digital trade policies, and
d) identify actionable lessons and priorities for ASEAN economies.

To inform these goals, we draw on data from the WRP, which captures perceptions of risk from over 125,000 respondents across low-, middle-, and high-income countries. We contribute fresh insights by integrating data on AI and data privacy risks with relevant databases on digital trade frameworks. We also triangulate and validate our findings through consultations with key policymakers and stakeholders in ASEAN.

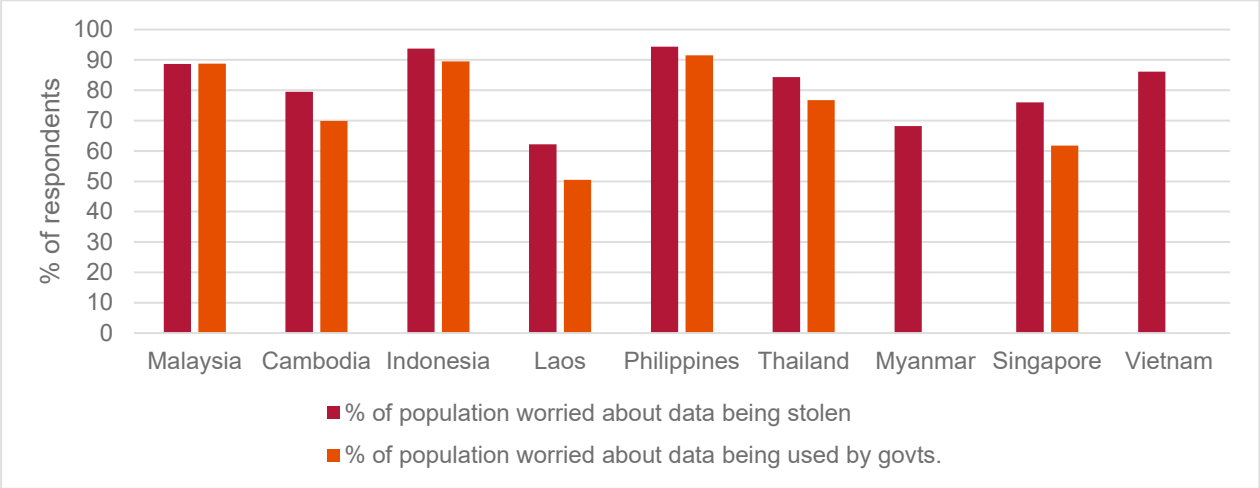
Key messages

1. There are significant but varied concerns on AI and data risks globally and within the ASEAN region

According to the WRP, over 80% of respondents in Malaysia, Indonesia, the Philippines, Thailand, and Vietnam are concerned about their data being stolen. In Malaysia, Indonesia, and the Philippines, a similar proportion also fears government misuse of personal data (Figure ES1). These concerns are compounded by increasing cyber threat, such as data breaches and fraud, which erode trust in digital transactions and hinder the growth of digital trade. The lack of harmonised data protection laws across ASEAN further exacerbates these issues, creating regulatory uncertainty for businesses operating across the region.

Attitudes toward AI vary significantly by income level and country. While over 45% of respondents in high-income countries believe AI will mostly help in the next 20 years, this figure drops below 35% in lower- and upper/middle-income nations. In ASEAN, countries like Thailand, Singapore, and Vietnam seem relatively optimistic, with a majority expecting AI to be beneficial. Conversely, Cambodia and Indonesia seem more cautious, with a larger share of the population fearing AI will do more harm than good over the next 2 decades.

FIGURE ES1. PERCENTAGE OF POPULATION WORRIED ABOUT THEIR PERSONAL INFORMATION



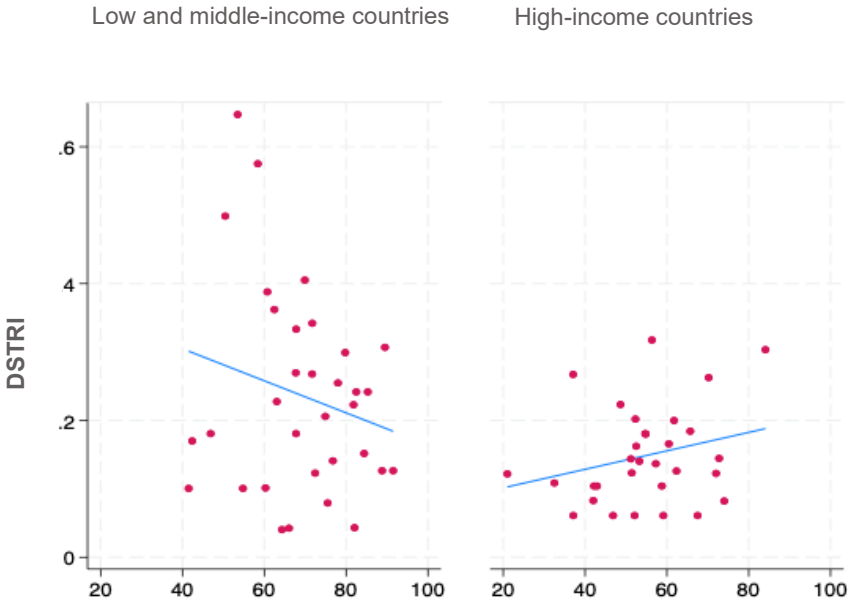
Source: Lloyd's Register Foundation (2021). World Risk Poll 2021.

2. Digital trade policy responses to rising digital risks tend to vary across the development levels of countries, with high-income countries responding by restricting the trade in digital services

Countries facing higher perceived data and AI risks tend to have higher Digital Services Trade Restrictiveness Index (DSTRI) scores, which measures the openness of the economy to digital services trade. A higher score indicates more restrictions on digital trade in services.

Looking across income levels, however, this relationship is evident for the sample of high-income countries but not for the low and middle-income ones. In the latter, higher data and AI risks are negatively correlated with the DSTRI. There are several possible reasons for this, including different levels of dependence of countries on foreign technologies, prioritisation of digital security according to national agendas, varying levels of trust in institutions, and differences in regulatory enforcement, digital advocacy, and public engagement in policymaking (Figure ES2).

FIGURE ES2. DIGITAL SERVICES RESTRICTIVENESS INDEX AND DATA RISKS, BY INCOME LEVEL, LMICS (LEFT) AND HICS (RIGHT)



Notes: DSTRI values (Y-axis) are represented as average values of the years 2019–21. The X-axis shows the percentage of the population worried about data being used by the government. HICs = high-income countries. LMICs = low and middle-income countries.

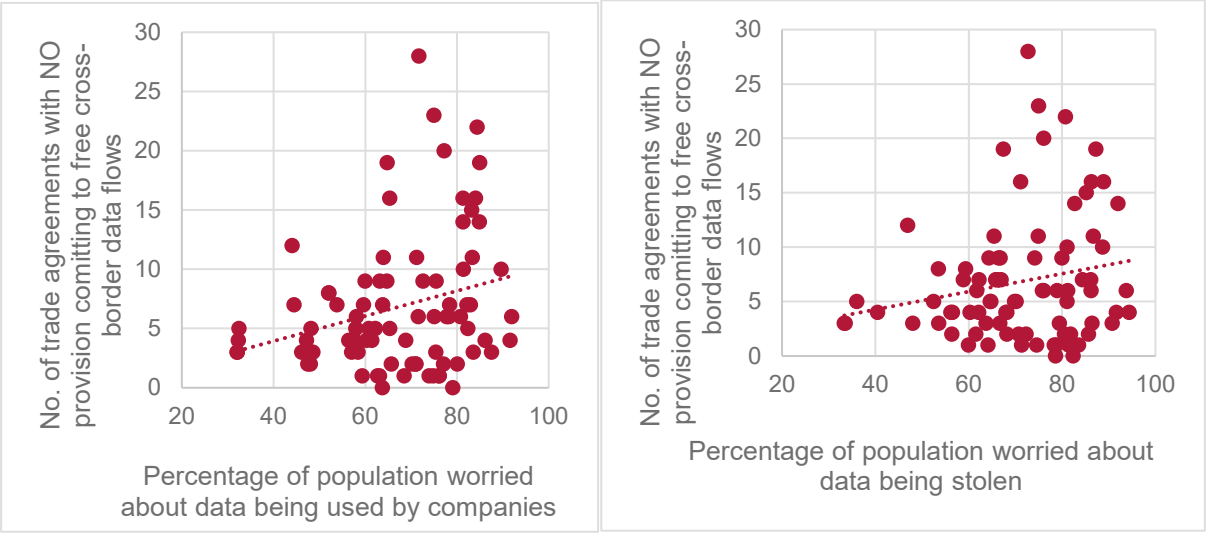
Source: Authors, based on Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

3. Countries with higher digital risks tend to preserve more policy space on data governance in digital trade agreements

Although there is a two-way relationship between perceptions of digital risks and digital trade regulations, we find a positive correlation between higher perceived data risks and participation in trade agreements that include a provision on digital trade or e-commerce provisions. These tend to be focused on data privacy, e-trade facilitation, and consumer protection.

Despite having stronger digital trade regulation, these countries often avoid committing to free cross-border data flows or banning data localisation. There is a positive correlation between countries' digital risks and participation in trade agreements that have NO provision committing to free cross-border data flows and NO bans on data localisation, meaning the country retains some flexibility to impose data localisation rules. Higher public concern over data misuse is positively linked to retaining flexibility in trade agreements, reflecting priorities around data sovereignty and economic security (Figure ES3).

FIGURE ES3. CROSS-BORDER DATA COMMITMENTS AND DATA RISKS



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; and Burri et al. (2022). TAPED data set.

4. ASEAN is fast progressing towards digital regulation but there is significant divergence in terms of data governance, cybersecurity, and e-commerce regulation

ASEAN is yet to implement any regulation or agreement concerning AI in digital trade, but almost all ASEAN members have a conditional flow regime when it comes to data, safeguarding privacy, and protecting personal data. There is a lack of harmonised cross-border data flow policies; the Philippines and Singapore allow a free flow of data across borders, with minimal regulatory requirements, while Indonesia and Vietnam have a restrictive approach, completely or partially restricting cross-border data flows for national and public security reasons.

Policy recommendations

1. *Embed a risk-based approach in digital trade agreements*

ASEAN should integrate risk considerations, such as public concerns around data misuse and AI harms, into the design of digital trade agreements. This includes creating flexible, tiered provisions for data governance and AI regulation that reflect varying national capacities and public risk perceptions, while still promoting regional harmonisation where feasible.

Cross-border policies that are less informed about the workings of generative AI technologies may be inefficient at regulating AI and data-related trade, potentially increasing the risk of data privacy violations and international legal disputes. Therefore, it is important for trade agreements to involve collaborations between countries on understanding AI-related developments and ethical concerns, to improve and evolve the terms of their agreements.

2. *Foster regional cooperation on AI standards and capacity-building*

While the Digital Economy Framework Agreement (DEFA) could play an important role in developing and aligning AI governance across ASEAN countries, a common regulatory framework on AI will be challenged by the existing digital divide between ASEAN members. Leading East Asia,

Singapore had an AI readiness score of 84.2 in 2024, while Myanmar, Cambodia, and Laos scored less than 40,[1] suggesting their policy prerogatives regarding AI will be different.

Given the digital divide within ASEAN, it is essential to support less digitally advanced members (e.g. Cambodia, Lao PDR, Myanmar) through regional initiatives focused on AI readiness. This can include shared technical standards, resource-sharing platforms, and ASEAN-wide capacity-building programmes to align national AI governance frameworks over time.

3. *Strengthen the ASEAN Guide on AI Governance and* Ethics *with actionable implementation tools*

The *ASEAN Guide on AI Governance and Ethics*, drafted in 2024, is a practical guide for organisations in the region that wish to design, develop, and use AI technologies. It provides guiding principles to help ensure trust in AI and in designing, developing, and deploying ethical AI systems. Guidelines for monitoring, auditing, and accountability in AI systems in the guide should address the needs and perspectives of AI actors and potential users in ASEAN countries.

To enhance its impact, ASEAN should supplement the guide with practical implementation tools such as monitoring frameworks, auditing guidelines, and country-level roadmaps. Incorporating context-informed methods like public consultations and landscape assessments will ensure that the guide reflects the diverse needs of Member States.

4. *Promote inclusive dialogue and collaboration on emerging technologies in trade policy*

In regulating AI, a common approach has been to adopt technical standards on AI as part of digital trade agreements, such as the Digital Economy Partnership Agreement between Chile, New Zealand, and Singapore (2020); the Australia–Singapore Digital Economy Agreement (2020); the UK–Singapore Digital Economy Agreement (2022); and the EU–Singapore Digital Partnership (2023).

ASEAN has established a working group on AI governance[2] that provides formal mechanisms on cooperation, including on generative AI. Such standing digital policy forums can facilitate ongoing, multi-stakeholder dialogue on emerging technologies. They can help to align trade policies with evolving technological realities, foster trust through transparency, and reduce the risk of cross-border legal disputes through informed cooperation.

[1] Oxford Insights (2024). AI readiness report 2024.
[2] The 4th ASEAN Digital Ministers' Meeting (Joint Media Statement 2023).

1. Introduction

With a rapidly expanding digital economy and increasing internet penetration, ASEAN countries can leverage digital trade to facilitate access to global markets and foster innovation. Digital trade can also transform the region by strengthening regional integration and enhancing the competitiveness of businesses, particularly micro-, small-, and medium-sized enterprises (MSMEs). Digital trade can be understood as encompassing digitally enabled transactions in goods and services that can be delivered digitally or physically, involving consumers, firms, and governments.[3] Building on this definition, the *Handbook on Digital Trade* provides a framework for measuring digital trade, defining it as "all international trade that is digitally ordered and/or digitally delivered".[4] Digitally ordered trade, in the handbook, refers to "the international sale or purchase of a good or service, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders". Digitally ordered trade is therefore equivalent to international e-commerce and a subset of total e-commerce. Digitally delivered trade, on the other hand, is defined as "all international trade transactions that are delivered remotely over computer networks".[5]

In 2021 the total ASEAN digital economy was valued at between $300 and $400 billion, and the ASEAN Digital Economy Framework Agreement (DEFA) is estimated to increase this figure sevenfold by 2030.[6] Digital trade in ASEAN is also sizeable; the annual value of business-to-consumer (B2C) e-commerce export revenue for the ASEAN-6 alone – Singapore, Malaysia, Thailand, Vietnam, Indonesia, and the Philippines – was estimated to be USD18.9 billion in 2023.[7] Thailand accounted for USD 6 billions of this figure, followed by Malaysia at USD4.6 billion, Vietnam at USD3.6 billion, Indonesia at USD3.1 billion, Singapore at USD1.3 billion, and the Philippines at USD0.3 billion.

However, there are significant disparities in the size of the digital economies, and digital trade, across ASEAN members. For instance, while Singapore's digital economy accounts for 17% of its GDP, Myanmar's pre-COVID digital economy was only 1–3% of its GDP.[8] This mixture of countries in ASEAN at different stages of digital development presents an important challenge in leveraging digital trade for development.

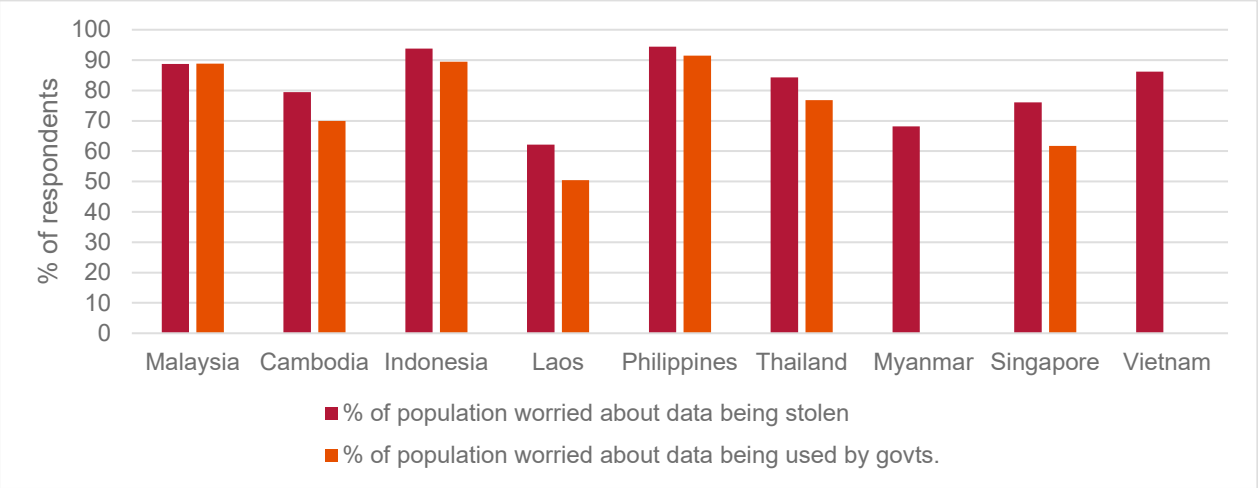
Several challenges hinder the full development and use of digital trade across the region, including regulatory and policy fragmentation, digital infrastructure gaps, digital literacy, logistics, financial inclusion, and payment system barriers. But beyond the traditional challenges to digital development – the high costs of internet connectivity, digital skills, and lagging digital infrastructure – threats to data security and data privacy have emerged as a new and prominent challenge facing digital economies. Rising cyber threats, including data breaches and fraud, undermine consumer trust in digital transactions, potentially limiting digital trade. Worries about overuse or misuse of

---

[3] López González, J. and M. Jouanjean (2017). OECD Trade Policy Papers, No. 205, OECD Publishing, Paris.
[4] Organisation for Economic Co-operation and Development (OECD) (n.d.). Digital Services Trade Restrictiveness Index.
[5] Furthermore, the concept of digitally delivered trade, which, by definition, only covers services, is, in practice, equivalent to the concept of service supply via Mode 1 – that is, services that are digitally delivered are most likely supplied via Mode 1.
[6] Study on the ASEAN Digital Economy Framework Agreement (Aus4ASEAN and BCG, 2024).
[7] Kaul, A., Lim, M. and Brahmecha, A. (2024). Transforming trade: The e-commerce revolution in ASEAN. Access Partnership.
[8] Country commercial guides, Digital Economy (ITA, 2024).

personal information have also been rampant in ASEAN economies because of the inconsistent data protection laws, which have created regulatory uncertainty for businesses operating in multiple ASEAN markets. In a survey of digital consumers in five ASEAN markets – Thailand, the Philippines, Malaysia, Indonesia, and Singapore – more than half of the respondents across all markets expressed concerns about the increasing likelihood of online fraud and hacking, with 43% of respondents in Indonesia and 34% in Malaysia saying they were very worried about becoming fraud victims.[9] The survey also found that over 30% of respondents in each market were "very concerned" about sharing their private data online.[10] These findings are echoed in the WRP; over 80% of the population in the ASEAN economies of Malaysia, Indonesia, the Philippines, Thailand, and Vietnam are worried about their data being stolen (Figure 1). In Malaysia, Indonesia, and the Philippines, over 80% of the population are also worried about their data being used by governments.

FIGURE 1. PERCENTAGE OF POPULATION WORRIED ABOUT THEIR PERSONAL INFORMATION



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021.

The economic losses from data breaches in ASEAN rose by $0.18 million between 2022 and 2023, with Singapore seeing a 174% surge in phishing attempts, and cyber-attack costs rising to more than $4.5 billion in Indonesia.[11] The risk is particularly pernicious for small firms: a digital divide survey in ASEAN found that only 68.5% of small firms have adopted cybersecurity software.[12] Such vulnerabilities keep the digital sectors from being robust, limiting digital transactions and consumer uptake of new technologies and therefore constraining digital trade growth.

Concerns around the development implications of AI have also increased in ASEAN countries. A global study of outlooks for 2025 by Ipsos found that 85% of those surveyed in Indonesia, 81% in the Philippines, 67% in Singapore, and 73% in Malaysia found it likely that AI would lead to many new jobs being lost in their country.[13] In another survey conducted across Malaysia, the Philippines,

[9] GSMA (2024). Consumer attitudes toward fraud and opportunities for mobile network operators in SEA.
[10] GSMA (2024).
[11] Mahusin, H. and Prilliadi, F. (2024). Strengthening ASEAN Cybersecurity. Jakarta: Economic Research Institute for ASEAN and East Asia (ERIA).
[12] Kasih, M.C. (2023). Fostering ASEAN's Digital Future through Cybersecurity Policies and Human Empowerment. ERIA Policy Brief 2023-02.
[13] Ipsos (2024). Ipsos predictions 2025 report.

Singapore, and Vietnam, as well as Australia and India, data privacy and misinformation issues related to AI technologies emerged as big concerns. Roughly 59% of respondents identified "deepfakes" – AI-generated content manipulating real content – as the emerging technological development they were most afraid of.[14] Cybersecurity threats, involving fake news and disinformation, are also prominent in the region because of inadequate regulatory measures, with the exception of Singapore's Protection from Online Falsehoods and Manipulation Act of 2019.[15]

Bridging the digital divide will require coordinated policies, strategic investments in digital infrastructure, and comprehensive capacity-building initiatives to ensure inclusive digital trade across the region. As ASEAN navigates the challenges of COVID-19, an uncertain recovery, and rising global geopolitical tensions, regional cooperation is even more crucial.

For this reason, our policy brief focuses on a) understanding the challenges of digital trade in ASEAN; b) mapping the fragmentation of the digital trade policy framework; and c) identifying lessons/priorities for ASEAN economies on digital trade policy. To do so, we leverage Lloyd's World Risk Poll (WRP), which gathers information on risks for over 125,000 respondents across low-, middle-, and high-income countries. We contribute new insights by integrating data on AI and data privacy risks from the WRP with relevant databases on digital trade frameworks and validating findings through consultations (see Appendix A). We do this with a view to informing interventions in key policy areas on digital trade that have the potential to improve lives and/or make people feel safer. This policy brief is part of a larger project on the WRP, which aims to inform policymakers about critical risk areas in digital technology policy (focusing on AI), digital economy and trade agreements, industrial policy, and labour policy. The regional focus of the project is Southeast Asian countries, although insights from a global perspective are shared.

Section 2 examines the digital trade divide across and within ASEAN economies. Section 3 provides a comprehensive overview of the digital trade policy frameworks in the region, with Section 4 focusing on AI in digital trade policy. Sections 5 and 6 provide new analysis using information from the WRP on data and AI risks, respectively. Section 7 concludes with global and ASEAN-specific policy recommendations.

[14] Kaspersky (2020). Digital reputation economy report.
[15] Putra, B. A. (2024). Governing AI in Southeast Asia: ASEAN's way forward. Frontiers in Artificial Intelligence, 7. doi:10.3389/frai.2024.1411838.

2. Digital trade divide in ASEAN

2.1 Digital divide across countries

In ASEAN, the uptake and use of the internet has been rapid, reaching 94% of the population in Singapore, 98% in Malaysia, and 99% in Brunei Darussalam.[16] Although it remains lower in newer Member States, such as Cambodia (57%), Lao PDR (66%), Myanmar (44%), and Indonesia (69%), growth in use since the year 2000 has been considerable across all countries.[17] While there is a strong potential in the region to develop digital trade, the quality of the internet has been varied. For instance, in 2023 the fixed broadband internet speed ranged from above 200 megabits per second in Singapore and Thailand, to less than 100 in the Philippines and Brunei Darussalam, and less than 50 megabits per second in Lao PDR, Cambodia, and Myanmar.[18]

Since digital trade relies on logistics, the costs, quality and capacity for logistical services are important indicators of digital trade capacity. A significant inequality is noted between countries in ASEAN on the World Bank's Logistical Performance Index; as of 2023, Singapore had an LPI score of 4.3, followed by the Philippines and Vietnam (3.3), and Cambodia and Lao PDR (2.4). High logistical costs are also a key challenge to digital trade in Vietnam; in a survey of Vietnamese MSMEs engaging in e-commerce, 94% of firms believed that the high costs of cross-border logistics were hindering their use of e-commerce to export goods.[19]

2.2 Digital divide within countries

Within ASEAN economies, some sectors and types of firm are ahead in their adoption of digital trade. And ASEAN SMEs adopt relatively simple digital technologies, such as web pages, to varying degrees across sectors: in Cambodia 41% of firms in the hospitality and tourism sector have a web page, compared to only 13% in manufacturing,[20] and only 22% of firms outside the core ICT industries in the Philippines have a web presence.[21] A phone survey of MSMEs in ASEAN found that micro and small companies have lower adoption of technology tools than medium and large companies.[22] The study further found a disparity in institutional support, with industrial associations and government public institutions providing more support to larger businesses than smaller ones, constraining digital tool adoption in small business (ibid.). MSMEs remain under-represented in the e-commerce revenue share, earning between 22% and 54% of the overall B2C e-commerce export revenue today.[23]

---

[16] Internet penetration data (World Development Indicators, 2024).
[17] Box, S. and Lopez-Gonzalez, J. (2017). The future of technology: Opportunities for ASEAN in the digital economy, ResearchGate.
[18] Sefrina, S. (2024). An inclusive digital economy in the ASEAN region. Economic Research Institute for ASEAN and East Asia (ERIA).
[19] Kaul et al. (2024). Transforming trade: The e-commerce revolution in ASEAN, Access Partnership.
[20] López González, J. (2019). Fostering participation in digital trade for ASEAN MSMEs, OECD Trade Policy Papers, No. 230, OECD Publishing, Paris.
[21] Philippines Statistics Authority (2022). Survey on ICT.
[22] Oikawa et al. (2024). The digital divide amongst MSMEs in ASEAN, Economic Research Institute for ASEAN and East Asia (ERIA).
[23] Kaul et al. (2024). Transforming trade: The e-commerce revolution in ASEAN, Access Partnership.

Gender inequalities in digital access can also translate into digital inequalities in the adoption of digital trade. The percentage of female internet users has been consistently lower than the percentage of male internet users in all ASEAN countries for which data has been available between 2019 and 2023, with the exception of the Philippines in 2022.[24] Gender inequalities persist despite educational opportunities; a study across ASEAN countries found that most women who study technology-related courses take up careers that are not technology-focused.[25] Women entrepreneurs also face disparities with male entrepreneurs in the digital economy. For example, a study on women and e-commerce in Southeast Asia found that in Indonesia, only 32% of businesses in e-commerce in 2020 were women-owned, and women-owned businesses contributed just 36% to the total gross margin value in the sector, a fall from 43% in 2019.[26] The gender gap in digital skills access clearly also translates into a gap in abilities to employ digital tools in enterprises. In a study in Malaysia, over 80% of micro and small women entrepreneurs (MSWEs) surveyed agreed that digital technology was essential for increasing business flexibility, accelerating processes and accessing information, but only around 60% of MSWEs stated that they used social media for their businesses, only 63.5% reported having the knowledge to resolve technical issues, and only 64% reported having the knowledge to protect their enterprises' digital content and assets.[27]

Ethnic marginalisation also accounts for digital divides. A qualitative study in Malaysia found multiple challenges of physical access, skill deficiencies, and cultural divisions, among others, faced by native communities in the state of Sabah when adopting ICTs.[28] A study in Vietnam found that even as mobile phone ownership has seen tremendous growth, ethnic minorities lag behind in phone adoption.[29] These inequalities imply that different population segments within countries have varying abilities to engage with the digital economy.

The shortage of skilled labour in the digital economy is another significant concern. In the study of MSMEs across ASEAN, 72% of the web-surveyed businesses reported that employees were not keen to adopt ICTs, as they found digital tools confusing and increased the work process; 80% reported that employees were unable to use digital tools because of limited skills; and 49% said there was no customer support available in the country or region.[30]

---

[24] World Bank (2025). *World Development Indicators*. Washington, DC: World Bank. Available at: https://databank.worldbank.org/source/world-development-indicators (accessed: 15 January 2025).
[25] Rastogi et al. (2024). Closing tech's gender gap in Southeast Asia. Boston Consulting Group.
[26] International Finance Corporation (IFC) (2021). Women and e-commerce in Southeast Asia.
[27] The Asia Foundation (2024). Striving digitally: Understanding the challenges of Malaysian women entrepreneurs.
[28] Fang, Y., Gill, S., Kunasekaran, P., Rosnon, M.R., Talib, A. and Aziz, A. (2022). Digital divide: An inquiry on the native communities of Sabah. *Societies*, 12(6), p. 148. doi:10.3390/soc12060148.
[29] Kaila, H. (2023). Ethnic digital divide? Evidence on mobile phone adoption. *Applied Economics*, 55, pp. 1–15. doi:10.1080/00036846.2022.2103502.
[30] Oikawa et al. (2024). The digital divide amongst MSMEs in ASEAN, Economic Research Institute for ASEAN and East Asia (ERIA).

3. Digital trade policy

Within expanding digital trade, and a widening digital trade divide, the issue of governance emerges as critical. Negotiations on digital trade rules are taking place in multiple forums across international, continental, regional, and national levels. The World Trade Organization (WTO) Work Programme on E-commerce, established in 1998, provides a framework for discussions on trade-related aspects of e-commerce. It explores issues such as digital trade facilitation, data flows, cybersecurity, electronic contracts, and consumer protection. But there has been a lack of consensus between developed and developing countries at the WTO, leading to a subset of 91 countries, including Brunei Darussalam, Cambodia, Lao PDR, Malaysia, Myanmar, and Singapore, agreeing "to commence WTO negotiations on trade-related aspects of electronic commerce".[31] The majority of the participating members are developed countries, with only five least-developed countries (LDCs) participating. In 2024 a stabilised text of the E-Commerce Joint Initiative (JSI) was announced, which established a consensus on some of the less contentious digital trade issues, such as electronic trade facilitation, open government data, online consumer protection, personal data protection, and cybersecurity.

3.1 Bilateral and regional FTAs

A more ambitious digital trade agenda has been largely pushed forward through bilateral and regional FTAs and stand-alone digital economy agreements (DEAs), which establish rules on cross-border data flows, data localisation, digital trade facilitation, and source code sharing. Three distinct types of approach on data governance are evident across key players – the USA, the EU, and China. The USA follows a market-driven model, relying on industry self-regulation and sectoral laws like the California Consumer Privacy Act rather than a comprehensive federal framework, giving businesses greater flexibility.[32] The EU prioritises data protection through the General Data Protection Regulation (GDPR), which enforces strict user rights, consent requirements, and cross-border data transfer restrictions to safeguard privacy.[33] Meanwhile, China adopts a national security-driven model, with laws like the Personal Information Protection Law and the Cybersecurity Law emphasising state control, data localisation, and surveillance to maintain government oversight and social stability.[34] These different frameworks demonstrate how nations balance economic interests, individual rights, and state security in data governance.

Many modern preferential trade agreements (PTAs), such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP), now include digital trade chapters that set rules on e-commerce, data flows, and digital taxation. The CPTPP is a pioneering trade agreement that shaped subsequent trade agreements such as the RCEP, the United States–Mexico–Canada Agreement (USMCA), and the Singapore–Korea and UK–Singapore DEAs, among others. The RCEP is not subject to dispute settlement, and the USMCA goes beyond the CPTPP by bringing intermediary liability rules.

---

[31] Joint Statement on Electronic Commerce (WTO, 2019).
[32] Schwartz, P. M. (2019). Global data privacy: The EU way. *New York University Law Review*, 94, pp. 771–814.
[33] Voigt, P. and Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. doi:10.1007/978-3-319-57959-7.
[34] Escobar, E.F.-N. (2025). How do the European Union's GDPR and China's PIPL regulate cross-border data flows?. International Policy Review.

In terms of regional and bilateral trade agreements with digital provisions, of the 346 PTAs that came into force between 2000 and 2019, 184 contain provisions that are relevant to digital trade, with 108 having specific e-commerce provisions and 78 having dedicated e-commerce chapters.[35] PTAs with digital trade provisions accounted for 61% of all such agreements concluded between 2010 and 2018, and two-thirds of WTO members were party to a PTA with e-commerce provision.[36] Since January 2020, 49 agreements covering digital trade commitments have been concluded or signed, and more are being negotiated; digital trade provisions are increasingly contained in standalone chapters rather than in services and investment chapters; more digital trade commitments in PTAs have been negotiated; and "'digital economy agreements (DEAs)" have emerged.[37] A DEA can be thought of as DTA-plus, covering a more ambitious set of digital provisions, essentially mainstreaming "digital" into areas such as financial services and trade facilitation.

3.2 Digital trade policy fragmentation in ASEAN

The stagnating growth of intra-ASEAN trade, combined with external technological advancements, prompted Member States such as Singapore to spearhead the new economic Digital Economy Partnership Agreement (DEPA) formed among Chile, New Zealand, and Singapore. The DEPA establishes common aspirations to promote, for example, digital interoperability and inclusion. ASEAN countries are also part of several regional initiatives to set policy frameworks to govern digital trade; a framework for developing the DEFA (I) was adopted in September 2023 at the 43rd ASEAN Summit, with negotiations expected to be concluded by 2025. In addition, stand-alone DEAs, like the Singapore-led agreements with Australia, Chile, and South Korea, go beyond traditional trade deals by establishing deep cooperation on digital trade governance, data sharing, and emerging technologies. Studies have shown that such DEAs can positively increase the output of the ICT sector, having downstream benefits for the business services and financial sector, increasing their output by an average of 6.78%.[38]

While as a bloc, ASEAN is fast progressing towards digital regulation, countries have significant divergence in terms of data governance, cybersecurity, and e-commerce regulation. There is a lack of harmonised cross-border data flow policies, with some countries enforcing data localisation laws that restrict digital trade and others promoting free cross-border data flows. Fragmented regulatory regimes and restrictions on information flows are major challenges to digital trade.[39] The Philippines and Singapore allow a free flow of data across borders, with minimal regulatory requirements, while Indonesia and Vietnam have a restrictive approach, completely or partially restricting cross-border data flows for national and public security reasons. Malaysia and Thailand allow cross-border data

[35] Burri, M. and Polanco, R. (2020). Digital trade provisions in preferential trade agreements: Introducing a new dataset. *Journal of International Economic Law*, 23(1), pp. 187–220. doi:10.1093/jiel/jgz044.
[36] Willemyns, I. (2020). Addressing digital services in PTAs: only convergence in the 11th Hour? In R. T. Hoffmann and M. Krajewski (eds), *Coherence and divergence in services trade law*. Berlin: Springer.
[37] Burri et al. (2024). The evolution of digital trade law: Insights from TAPED. *World Trade Review*, 23(2), pp. 190–207. doi:10.1017/S1474745623000472.
[38] Lim, J. Z., Toh, M.-H. and Xie, T. (2022). Impact of digital economy agreements on ASEAN development: Estimates from a CGE model. Conference papers 333441, Purdue University, Center for Global Trade Analysis, Global Trade Analysis Project.
[39] Suvannaphakdy, S. and Pham, T. (2023). Introduction. In *GVC Reconfiguration*. Singapore: ISEAS Publishing, pp. 1-4. doi:10.1355/9789815104127-003.

flows based on rigorous compliance requirements.[40] Table 1 summarises the different approaches to cross-border data governance in ASEAN.

TABLE 1. FRAGMENTATION OF CROSS-BORDER DATA GOVERNANCE POLICY IN ASEAN

Country	Act/Practice	Description
Malaysia	Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Malaysia has joined an agreement with binding commitments to open transfers of data across borders: the CPTPP (Art. 14.11).
Lao PDR	Lack of participation in agreements with binding commitments on data flows	Laos has not joined any agreement with binding commitments to open transfers of data across borders.
Cambodia	Lack of participation in agreements with binding commitments on data flows	Cambodia has not joined any agreement with binding commitments to open transfers of data across borders.
Indonesia	Indonesia–Australia Comprehensive Economic Partnership Agreement	Indonesia has joined an agreement with binding commitments to open transfers of data across borders: Indonesia–Australia Comprehensive Economic Partnership Agreement (Art. 13.11).
Brunei	Comprehensive and Progressive Agreement for Trans-Pacific Partnership	Brunei has joined an agreement with binding commitments to open data transfers across borders: the CPTPP (Art. 14.11).
Myanmar	Lack of participation in agreements with binding commitments on data flows	Myanmar has not joined any agreement with binding commitments to open transfers of data across borders.
Vietnam	Comprehensive and Progressive Agreement for Trans-Pacific Partnership	Vietnam has joined an agreement with binding commitments to open transfers of data across borders: the CPTPP (Art. 14.11). But the country has been given 5 years to comply with the requirement.

[40] Ibid.

Philippines	Lack of participation in agreements with binding commitments on data flows	The Philippines has not joined any agreement with binding commitments to open transfers of data across borders.
Thailand	Lack of participation in agreements with binding commitments on data flows	Thailand has not joined any agreement with binding commitments to open transfers of data across borders.
Singapore	Comprehensive and Progressive Agreement for Trans-Pacific Partnership	Singapore has joined agreements with binding commitments to open transfers of data across borders, as in the CPTPP (Art. 14.11), Singapore–Australia Free Trade Agreement (Ch. 14 Art. 13), Free Trade Agreement between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore (Art. 9.9), and the Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore [Art. 8.61-f(2)].
	Singapore–Australia Free Trade Agreement	
	Free Trade Agreement between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore	
	Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore	
	Singapore–Korea Digital Partnership Agreement	
	Singapore–EU Digital Partnership Agreement	

Source: Compiled from the Digital Trade Integration Database.

Table 2 shows the types of restrictive regulatory measure imposed by ASEAN economies on cross-border data flows, ranging from a conditional flow of data to a requirement for local data storage and processing. Almost all ASEAN members seem to follow the EU approach of a conditional flow regime, safeguarding privacy, and protection of personal data. The depth of commitment also matters: in small developing countries, there is a clear preference for facilitation provisions such as cooperation in South–South RTAs, which are soft commitments, around paperless trade and

transparency.[41] "Soft" commitments are not enforceable by the parties, rather including "best effort" provisions like those "recognising the importance of", "working towards", or "promoting" a certain objective. The ASEAN Member States of Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam are part of the RCEP agreement, which has an ambitious and detailed e-commerce chapter but is not enforceable by state–state dispute settlement.[42]

TABLE 2. REGULATIONS ON CROSS-BORDER DATA FLOWS IN ASEAN

Country	Conditional flow regime	Ban to transfer and local processing requirements	Infrastructure requirements	Local storage requirements	Lack of participation in trade agreement with binding commitments on data flows
Malaysia	x			x	
Lao PDR	x	x			x
Cambodia		x		x	x
Indonesia	x	x	x		
Brunei	x				
Myanmar	x				x
Vietnam	x	x	x		
Philippines	x				x
Thailand	x	x			x
Singapore	x				

Source: Compiled from the Digital Trade Integration Database.

[41] Gaitan G. L. (2020). Electronic Commerce in Trade Agreements: Experience of Small Developing Countries. Geneva: CUTS International, Geneva.
[42] Kelsey, J. (2020). Important differences between the final RCEP electronic commerce chapter and the TPPA and lessons for e-commerce in the WTO. Bilaterals.org.

4. AI in digital trade policy

The advent of artificial intelligence poses various challenges to consumers, businesses, and governments in the digital economy. AI has already had a significant impact on cross-border digital trade. For example, a study on a sample of 35,575 apps used in 84 countries between 2015 and 2020 found that AI had increased mobile phone app trade tenfold.[43] AI poses risks of large-scale data privacy violations in digital transactions; personalised data can be used to predict and exploit consumer behaviour, approximating users' willingness to pay to create monopolist price discrimination in markets with insufficient competition, or where personalised pricing is complex or lacking transparency. Uber's opaque algorithmic pricing model is an example of this.[44] Personal information can also be used for behavioural manipulation, making consumers choose products that are profitable for firms by making them seem more attractive.[45] In workplaces, using AI technologies to augment, or even replace, traditional management, including automating screening, ranking, and selecting, and monitoring employee movements, location, and productivity, may erode workers' abilities to exercise their fundamental rights.[46] Employers can also violate employees' privacy by monitoring off-duty behaviour, social media activity, and personal data such as medical records, monitoring fitness data or tracking intentions to become pregnant, among other things.[47]

The rapid rise of AI requires digital policies to be continuously formulated and updated to ensure responsible integration into digital trade. Cross-border agreements can play a crucial role in safeguarding consumers and workers across jurisdictions, addressing concerns that arise when AI-driven systems transcend national boundaries. A major challenge stems from corporate secrecy surrounding algorithm development, which can hinder transparency and accountability in AI usage. While intellectual property and trade secrets are often cited to limit AI auditing and assessment, such restrictions can obstruct necessary oversight and regulation.[48]

When AI-related harms occur in cross-border digital transactions, national laws and legal authorities face limitations in enforcing protections and providing redress beyond their own jurisdictions. This issue becomes even more complex when consumers engage with intermediary platforms, where sellers may be untraceable because of complex legal structures.[49] Without coordinated international regulations, affected parties may struggle to seek justice or compensation.

The growing interdependence of digital systems across nations also highlights the risks posed by regulatory fragmentation. A lack of harmonised cybersecurity standards can create vulnerabilities, allowing cyber threats, malware, and malicious tools to spread freely across borders. Inconsistent regulatory frameworks may leave critical gaps in global digital defences, making interconnected

---

[43] Sun, R. and Trefler, D. (2023). The impact of AI and cross-border data regulation on international trade in digital services: A large language model. NBER Working Paper No. w31925.
[44] Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), pp. 70–84.
[45] Acemoglu et al. (2023). Artificial intelligence and the future of work. NBER Working Paper No. 31872.
[46] Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), pp. 70–84.
[47] De Stefano, V. (2019). "Negotiating the algorithm": automation, artificial intelligence, and labor protection. *Comparative Labour Law & Policy Journal*, 41, p.15.
[48] Ada Lovelace Institute (2021). Technical methods for regulatory inspection of algorithms.
[49] Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), pp. 70–84.

systems more susceptible to cyber-attacks.[50] Furthermore, disparities in AI governance can lead to digital barriers, where fragmented regulations restrict data flows, limit access to AI-driven services, and impede technological innovation. Such obstacles increase operational complexities for businesses, forcing them to navigate conflicting regulatory requirements in multiple markets.[51]

Theoretically, as per the principle of technological neutrality under the WTO, new technologies like AI could come under the framework of the existing WTO law, such as the General Agreement on Trade in Services (GATS), which could help to establish the conditions under which members can impose restrictions on specific types or uses of AI technology.[52] However, several challenges exist: a) GATS was designed to regulate traditional trade and is not best suited to the complexities of AI flows, which often involve cross-border data flows and algorithmic decision-making; b) GATS can fall short of regulating AI, which operates at the intersection between services and intellectual property, as well as smart devices; c) given the geopolitical tensions around AI and semi-conductor chips, countries may prefer to regulate AI domestically; and d) there are already diverging regulatory approaches to AI governance (e.g. the EU's AI Act versus China's AI governance policies), and using GATS to regulate AI could force premature harmonisation.

A more common approach has been to adopt technical standards on AI as part of digital trade agreements, including the DEPA between Chile, New Zealand, and Singapore (2020); the Australia–Singapore Digital Economy Agreement (2020); and the more recent UK–Singapore Digital Economy Agreement (2022). Although these international AI standards are voluntary, substantial legal weight is conferred on them when they are cross-referenced in binding international trade treaties, as they could be used for norm-setting.[53] PTAs with provisions on AI generally seek to promote collaboration for the development and adoption of frameworks that support the trusted, safe, and responsible use of these technologies.

ASEAN is yet to implement any regulation or agreement concerning AI in digital trade. It released the *ASEAN Guide on AI Governance and Ethics* in 2024, a practical guide for organisations in the region that wish to design, develop, and use AI technologies. It provides guiding principles to help ensure trust in AI, and in designing, developing, and deploying ethical AI systems, including "accountability and integrity", "privacy and data governance", "human centricity", "security and safety", and "transparency and explainability".[54] But it is a non-binding guide, leaving the onus of AI regulation on Member States. While an common regulatory framework on AI can be developed under DEFA, it will be challenged by the existing digital divide between ASEAN members. Leading East Asia, Singapore had an AI readiness score of 84.2 in 2024, while Myanmar, Cambodia, and Lao PDR scored less than 40,[55] suggesting their policy prerogatives regarding AI will be different.

Bilaterally, some ASEAN Member States are more actively addressing AI in their cross-border digital trade policy. Singapore signed a DEA with Australia in 2020 and with the UK in 2022; both parties acknowledge that artificial intelligence will play an important role in the international economy and that cooperation between their governments in regulation is required to maximise the

---

[50] Marwala, T. (2023). The Fourth Industrial Revolution has arrived. Comments on Moll. *South African Journal of Science*, 119(1/2). doi:10.17159/sajs.2023/15429.
[51] Marwala, T. (2023). The Fourth Industrial Revolution has arrived. Comments on Moll. *South African Journal of Science*, 119(1/2). doi:10.17159/sajs.2023/15429.
[52] Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), pp. 70–84.
[53] Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, 39(1), pp. 70–84.
[54] ASEAN Guide on AI Governance and Ethics (ASEAN, 2024 p.3, p.2).
[55] Oxford Insights (2024). AI readiness report 2024.

technologies' benefits[56]. Specifically, the Australia–Singapore DEA (2020) calls for members to "*collaborate on and promote the development and adoption of frameworks that support the trusted, safe, and responsible use of AI technologies*", and recognises "*the importance of developing ethical governance frameworks for the trusted, safe and responsible use of AI technologies that will help realize the benefits of AI*". These and the Digital Economy Partnership Agreement between Chile, New Zealand, and Singapore in 2021 acknowledge that AI requires ethical and governance frameworks to be developed, and these need to be aligned with internationally recognised principles and guidelines[57]. Moreover, there is a developing understanding of the possible data privacy concerns and issues related to generative AI in trade agreements; the UK–Singapore DEA seeks cooperation on issues and developments relating to artificial intelligence, including the "*ethical use, human diversity and unintended biases, industry-led technical standards and algorithmic transparency*", "*joint deployment and test-bedding opportunities*", *and* "*opportunities for investment in and commercialisation of AI and emerging technologies*".

While other ASEAN nations are yet to take concrete measures to govern AI in cross-border trade, many Member States have adopted laws concerning digital privacy, including Myanmar's 2017 law Protecting the Privacy and Security of Citizens, Vietnam's Law on Cyber Information Security, and the 2012 Data Privacy Act in the Philippines. Importantly, the digital trade policy approaches of ASEAN Member States seem to contrast with their approach to AI; Singapore, Thailand, and the Philippines, meanwhile, have introduced laws that have aligned with the EU's GDPR since 2020.[58] ASEAN Member States refused to adopt the global governance framework of the EU's AI Act, claiming it was too quick.[59] As countries' policy approaches to cross-border trade in AI vary within political and socio-economic contexts, the link between their populations' perceptions of AI-related risks and countries' trade openness regarding AI is likely to differ. This is demonstrated by the different relationships between AI perceptions and digital services trade restrictiveness in high-income and low-income countries discussed in Section 5.4.

[56] UK–Singapore Digital Economy Agreement, 2022; Australia–Singapore Digital Economy Agreement 2020
[57] UK–Singapore Digital Economy Agreement, 2022; Australia–Singapore Digital Economy Agreement 2020; Digital Economy Framework Agreement, 2021
[58] Putra, B. A. (2024). Governing AI in Southeast Asia: ASEAN's way forward. *Frontiers in Artificial Intelligence*, 7. doi:10.3389/frai.2024.1411838.
[59] Wang, J. (2024). Southeast Asia artificial intelligence governance. LSE International Development Blog.

5. Data governance and digital trade

In the above sections, we discussed digital trade across and within countries, the increasing risks and challenges pertaining to digital trade, and diverging digital trade policies. In the next few sections, we will present new analysis on the correlation and association between digital risks and digital trade policy.

This section combines information on data risks from the World Risk Poll (WRP) with relevant indicators of digital trade, such as trade in digitally deliverable services, the Digital Services Trade Restrictiveness Index, and participation in trade agreements. A key finding from this analysis is that there is significant heterogeneity in both data risks and policy responses to rising data risks, across countries globally and within ASEAN.

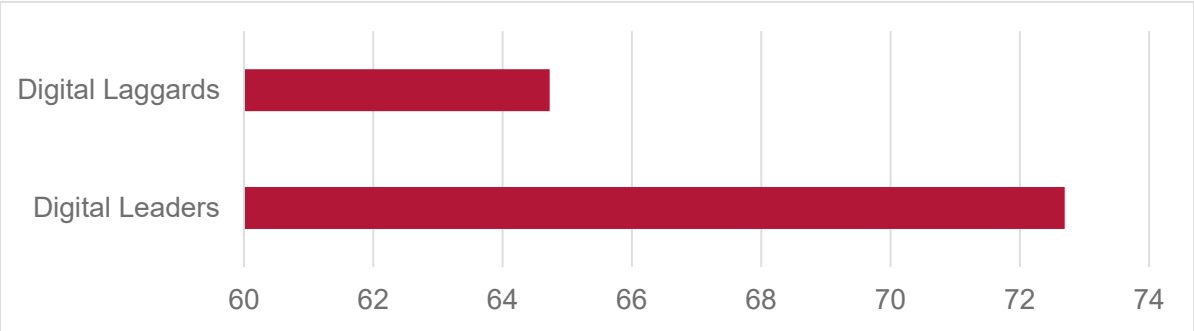
5.1 Data risks and digitally delivered services (DDS)

DDS refers to services that can be delivered remotely over computer networks, including insurance and pensions services, financial services, telecommunication, computer and information services, research, and development services. The DDS trade data set uses the definition of the IMF–OECD–UNCTAD–WTO *Handbook on Measuring Digital Trade*, which incorporates and builds upon the list of "potentially ICT-enabled services" identified by UNCTAD. From this data set, we identify "digital leaders" as countries in which the share of DDS exports is above the median level for the year 2021, and "digital laggards" as countries in which the share of DDS exports is below the median level for the year.

Correlating this with information in the WRP data reveals interesting findings. Figure 2 matches and merges the country-level information on data misuse in the WRP with country-level shares in global exports of DDS from the digitally delivered services trade data set[60] by the WTO. We find that a much higher share of the population of digital leaders – roughly 73% – are worried about their data being used by companies, compared to less than 65% of the population among the digital laggards.

[60] WTO data on digitally delivered services trade.

FIGURE 2. SHARE OF POPULATION WORRIED ABOUT DATA BEING USED BY COMPANIES, AVERAGE, BY DIGITAL INTEGRATION LEVELS OF COUNTRIES



Notes: T-tests confirm that the difference between digital laggards and digital leaders in terms of the share in global exports of DDS is statistically significant, at 1% level of significance, indicating both economic and statistical difference.

Source: Authors, based on Lloyd's Register Foundation (2021). World Risk Poll 2021; and WTO data.

5.2 Data risks and digital services restrictiveness

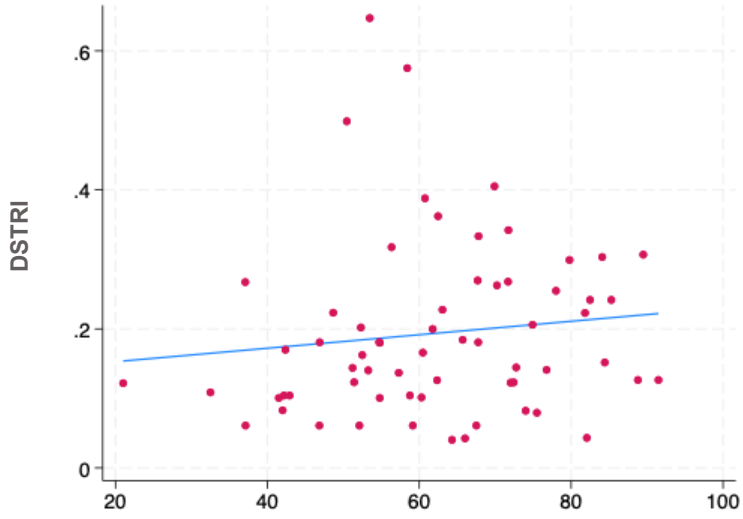
We also match and merge the country-level information on data risks from the WRP data set (for the year 2021) with the OECD's Digital Services Trade Restrictiveness Index (DSTRI). The DSTRI measures cross-cutting barriers that inhibit or prohibit firms' ability to supply services using electronic networks, regardless of the sector in which they operate. It includes restrictive measures[61] on five aspects:

a) Infrastructure and connectivity – restrictions related to interconnection on communication infrastructures and restrictions affecting connectivity (e.g. measures affecting cross-border data flows)
b) Electronic transactions – barriers affecting electronic transactions (e.g. non-recognition of e-signatures)
c) E-payment systems – measures that affect payments made through electronic means (e.g. restrictions on Internet banking)
d) Intellectual property rights – measures of domestic policies related to the protection and enforcement of trademarks, copyright, and related rights
e) *Other barriers* to trade in digitally enabled services – measures of barriers to trading in digitally enabled services that do not fall under the previous policy areas (e.g. performance requirements, limitations on downloading and streaming, or restrictions on online advertising).

It is a composite index that takes values between 0 and 1, where 0 indicates an open regulatory environment for digitally enabled trade and 1 indicates a completely closed regime. In Figure 3 we see that countries with higher data risks tend to have a higher DSTRI – that is, countries with higher data risks appear to be more closed to digital trade in services.

[61] https://goingdigital.oecd.org/en/indicator/73

FIGURE 3. DIGITAL SERVICES TRADE RESTRICTIVENESS INDEX (DSTRI), BY DATA RISK



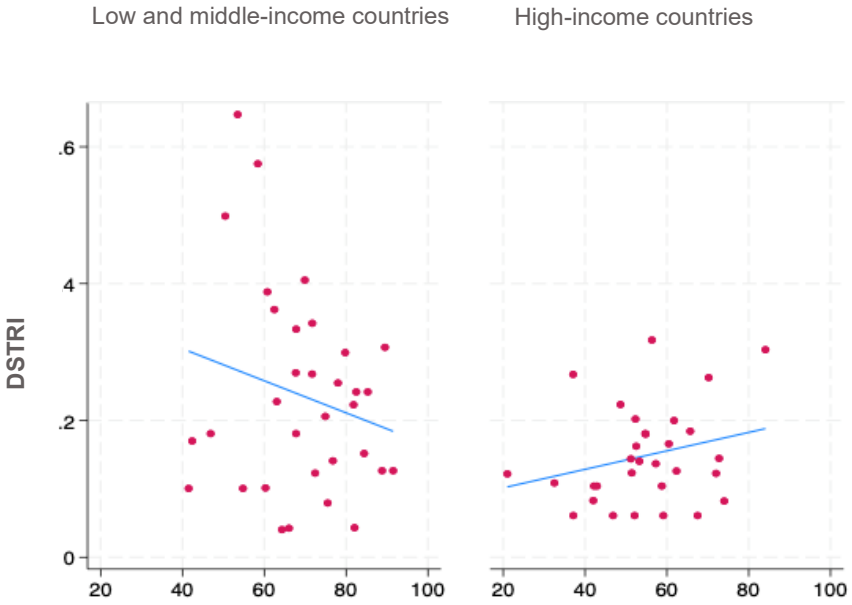
Note: The relationship between perceptions of digital risks and digital regulations is likely to be two-way, with one affecting the other. Figure 3 makes no assumptions about causation between the two variables. It shows a positive correlation, indicating that as variable X (percentage of population worried about data) increases, variable Y (DSTRI) increases.

Source: Authors, based on Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

However, looking across income levels, this relationship is evident for high-income countries but not for low and middle-income countries (Figure 4). In low and middle-income countries (LMICs), higher data risks are negatively correlated with the DSTRI (Figure 4, left). One possible reason for this is the differences between countries in their approach to data governance. Some high-income countries, particularly those in the EU, have adopted a data sovereignty approach to navigate data risks. Such policies prioritise data privacy and the digital security of citizens by restricting digital services trade or allowing such trade under certain conditions and safeguards. Developing economies, on the other hand, tend to depend on foreign providers for imports of digital services such as cloud computing, e-commerce platforms, and financial services. Despite high data risks, such countries may choose to be more open to the digital trade in services to access global markets and technologies and attract foreign investment that could grow the domestic capacity of this sector. It could also be the case that low-income countries, with little political or economic leverage in international negotiations, face higher pressure from international organisations, negotiating bodies, and corporations to remain open to digital trade.

Another reason for the difference in responses to data risks across developed and developing countries could be the differences in regulatory capacity and enforcement. In developed economies, there tends to be higher trust in institutions, stronger regulatory infrastructure, and technical capacity to impose and enforce stricter data protection measures (captured in the higher DSTRI). However, developing economies, particularly low-income countries, lack the regulatory and monitoring capacity to implement and enforce strict data policies.

FIGURE 4. DIGITAL SERVICES RESTRICTIVENESS INDEX AND DATA RISKS, BY INCOME LEVEL, LMICS (LEFT) AND HICS (RIGHT)



Notes: DSTRI values (Y-axis) are represented as average values of the years 2019–21. The X-axis shows the percentage of the population worried about data being used by the government. HICs = high-income countries. LMICs = low and middle-income countries.

Source: Authors, based on Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

5.3 Data risks and digital trade regulation

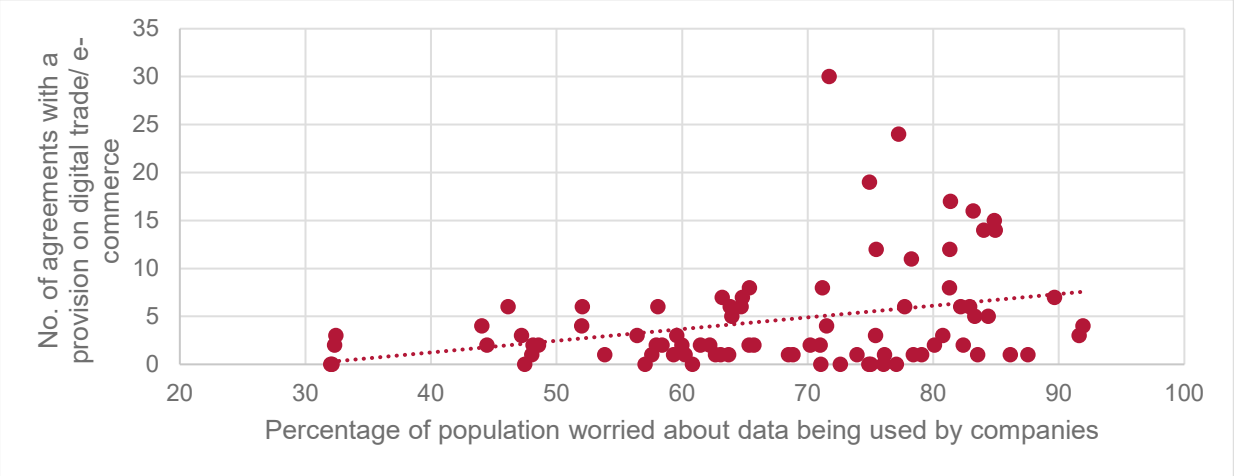
Perceptions about data risks can also shape a country's stance in digital trade regulations. In this section, we match and merge information from the TAPED (Trade Agreement Provisions on Electronic-commerce and Data) dataset[62] on countries' participation in trade agreements with digital trade provisions to data and AI risks from the WRP. The TAPED data set seeks to comprehensively trace developments in digital trade governance. It includes detailed mapping and coding of over 465 PTAs since 2000, covering chapters, provisions, annexes, and side documents that directly or indirectly regulate digital trade. From this data set, we extract information on: a) participation of countries in a trade agreement with a digital trade provision; b) participation in a trade agreement with a provision on cross-border data flow; and c) participation in a trade agreement with a ban on data localisation. We restrict data to trade agreements currently in force (which removes those currently being negotiated, such as the AfCFTA digital trade protocol).

Figure 5 shows a positive correlation between the percentage of the population that is worried about data being used by companies and the digital trade preparedness of countries, measured by the number of trade agreements a country is party to, which has a provision on digital trade/ e-commerce. Countries with higher data risks tend to participate more in trade agreements that have

[62] Burri et al, TAPED: Trade Agreement Provisions on Electronic Commerce and Data, available at: https://unilu.ch/taped.

a provision on digital trade/e-commerce. Most commonly, these provisions are on safeguarding data privacy and the personal data protection of consumers, the facilitation of e-trade, and online consumer protection.[63]

FIGURE 5. DIGITAL TRADE REGULATORY PREPAREDNESS



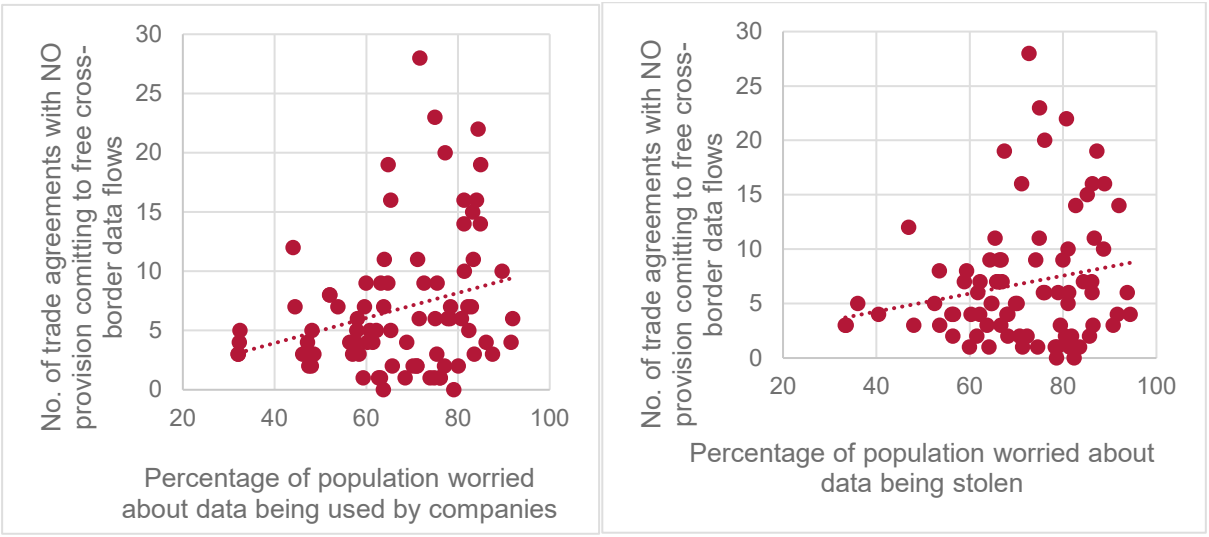
Note: The relationship between perceptions of digital risks and digital regulations is likely to be two-way, with one affecting the other. Figure 5 makes no assumptions about causation between the two variables. It shows a positive correlation, indicating that as variable X (percentage of population worried about data) increases, variable Y (participation in digital trade agreements) increases.

Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; and Burri et al. (2022). TAPED data set.

Interestingly, we note that while countries worried about data risk tend to be more prepared in terms of digital trade regulation, they tend to preserve more "policy space" in trade agreements on cross-border data flows. Figure 6 shows that countries with a higher percentage of the population worried about data being used by companies (left), or stolen (right), have a higher number of trade agreements with NO provision committing to free cross-border data flows. Similarly, in Figure 7 we see that countries with a higher percentage of the population worried about data risks tend to have a higher number of agreements with NO bans on data localisation, meaning the country retains some flexibility to impose data localisation rules. The importance of retaining the "right to regulate" the digital economy and policy space was echoed during consultations with ASEAN policymakers, as was the need to integrate digital trade rules in trade policy at their own pace.

[63] Banga et al. (2021). Digital Trade Provisions in the AfCFTA: what can we learn from South-South trade agreements. Supporting Economic transformation (SET) working paper series. ODI, London.

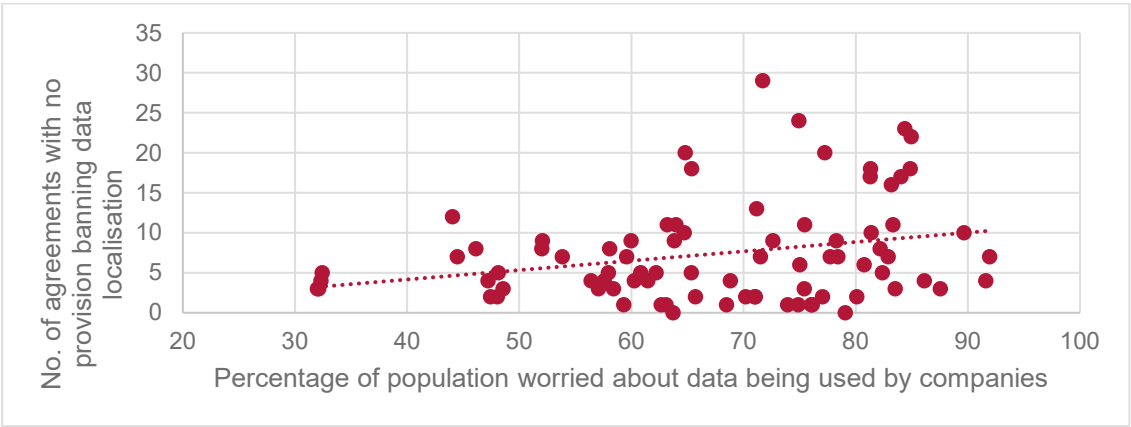
FIGURE 6. CROSS-BORDER DATA COMMITMENTS AND DATA RISKS



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; and Burri et al. (2022). TAPED data set.

The positive correlation between worries about data being used by companies and maintaining "policy space" on cross-border data flows in trade agreements can be understood in the context of national interests, data sovereignty, and economic security. As concerns grow about data misuse, governments want to ensure that international trade agreements give them the flexibility to regulate how data is handled, shared, and protected, preventing foreign companies from exploiting domestic data without oversight. In trade negotiations, developing countries like Indonesia, South Africa, and India have expressed concerns over premature rule-making and the desire to maintain policy space to regulate cross-border data flows. Policy space refers to the ability of a country to adopt and implement policies in its own national interest without being constrained by international trade agreements. In the context of data flows, maintaining policy space means a country retains the flexibility to regulate, restrict, or localise data as it sees fit.

FIGURE 7. DATA LOCALISATION COMMITMENTS AND DATA RISKS



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; and Burri et al. (2022). TAPED data set.

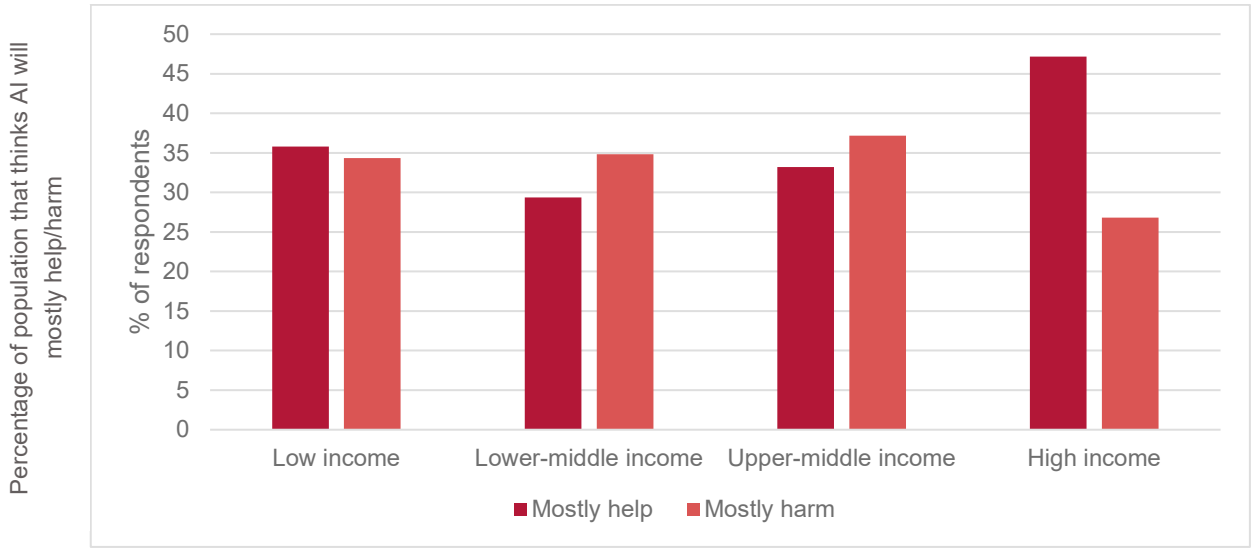
6. AI governance and digital trade

This section combines information on AI risks from the World Risk Poll (WRP) with relevant indicators of digital trade. A key finding from this analysis is that, like data risks, there is significant heterogeneity in both AI risks and policy responses to rising AI risks, across countries globally and within ASEAN.

As per data in the Lloyd's WRP survey, Figure 8 shows that over 45% of the population sampled in high-income countries perceive that AI will mostly help in the next 20 years. This falls to less than 35% in lower and upper-middle income countries. Similarly, the percentage of the population that perceives AI will be harmful over the next 20 years is much lower in high-income countries than others. The ability to use AI is associated with trust in AI tools, as evidenced by a study that found that individuals with less ability to use AI were more sceptical about it.[64] The higher proliferation of AI in the socio-economy in low- and middle-income countries implies a rise in suspicion of AI because of an inability to engage with it, while in high-income countries, a higher proliferation of AI implies greater engagement with it, and therefore fewer fears.

Focusing on ASEAN in Figure 9, we see that Thailand, Singapore, and Vietnam emerge with a positive outlook on AI; the majority of the population sampled in the countries think AI will help in the next 20 years. In contrast, Cambodia and Indonesia appear to have a more conservative outlook towards AI, with a higher share of the population worrying that AI will mostly harm the population in the next 20 years compared to the percentage that thinks AI will be helpful.

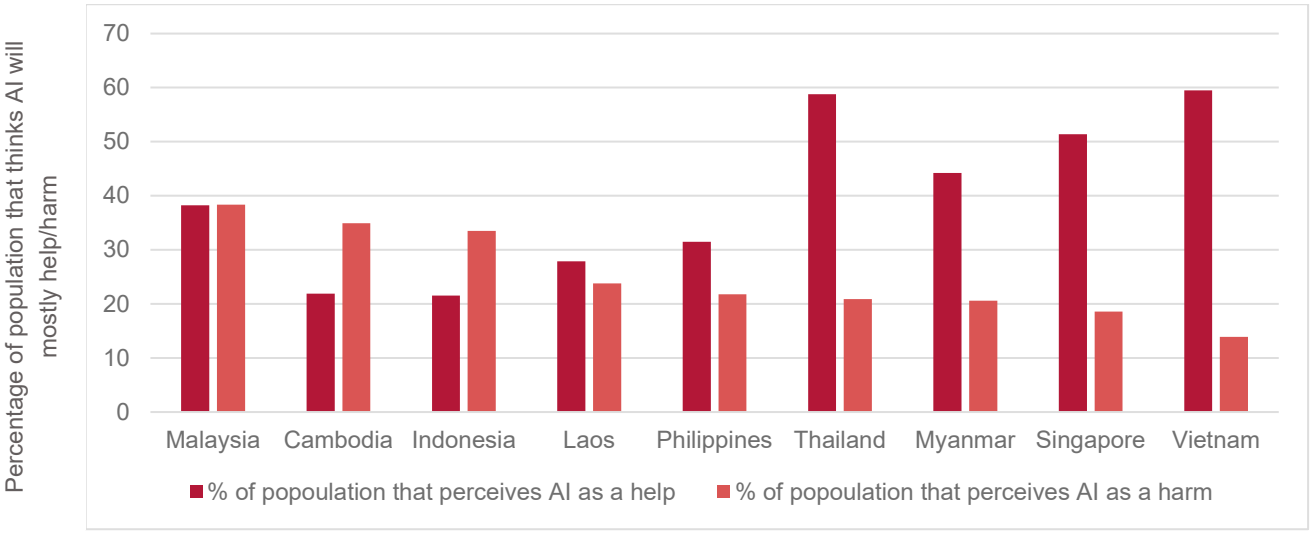
FIGURE 8. PERCEPTION OF AI RISKS IN THE NEXT 20 YEARS



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021.

[64] Huang, K.T. and Ball, C. (2024). The influence of AI literacy on user's trust in AI in practical scenarios: a digital divide pilot study. *Proceedings of the Association for Information Science and Technology*, 61(1), pp. 937–939.

FIGURE 9. PERCEPTION OF AI RISKS IN THE ASEAN IN THE NEXT 20 YEARS

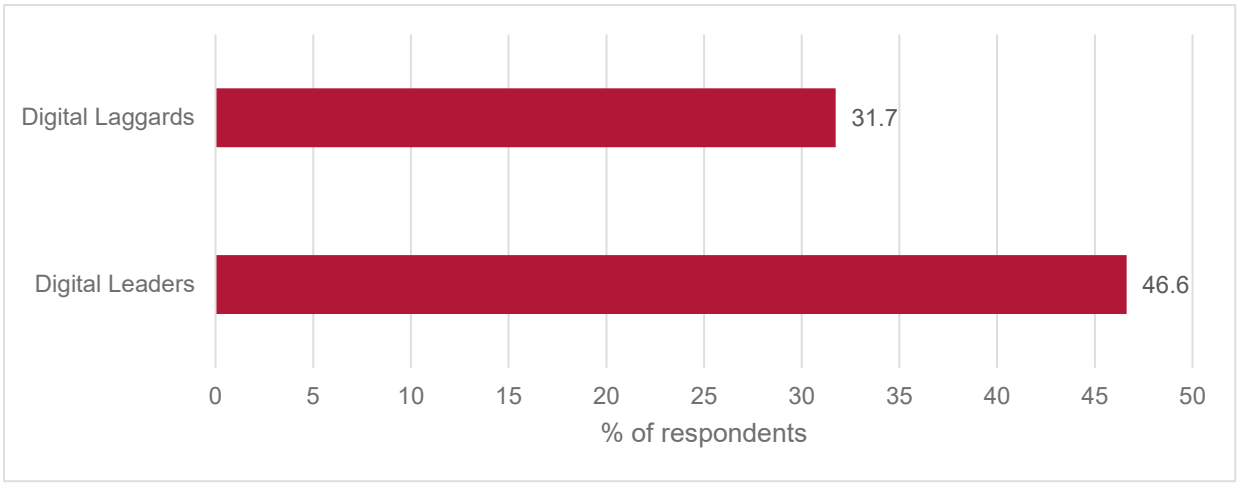


Source: Lloyd's Register Foundation (2021). World Risk Poll 2021.

6.1 AI risks and digitally delivered services (DDS)

Correlating AI risks from the WRP with WTO data on DDS reveals interesting findings. Figure 10 matches and merges the country-level information on data misuse in the WRP with country-level shares in global exports of DDS from the digitally delivered services trade data set by the WTO. We find that a significantly higher share of the population among digital leaders – roughly 47% – perceive AI will be beneficial over the next 20 years, compared to less than 32% of the population among the digital laggards.

FIGURE 10. SHARE OF POPULATION THAT PERCEIVES AI WILL BE BENEFICIAL IN THE NEXT 20 YEARS, AVERAGE, BY DIGITAL INTEGRATION LEVELS OF COUNTRIES



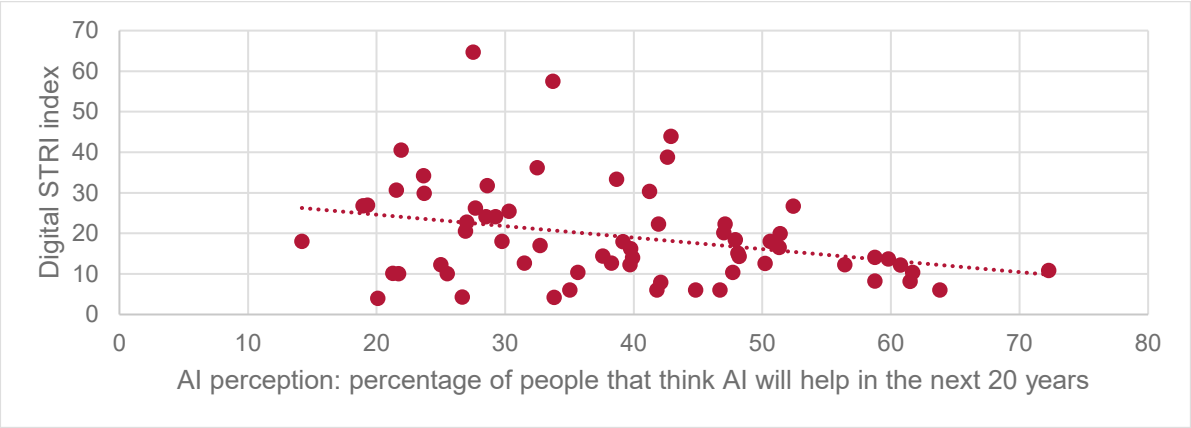
Notes: T-tests confirm that the difference in the share of global exports of DDS between digital laggards and digital leaders is statistically significant, at 1% level of significance, indicating both economic and statistical difference.

Source: Lloyd's Register Foundation (2021). World Risk Poll 2021 and WTO data.

6.2 AI risks and DSTRI

Matching and merging country-level information on AI risks from the WRP data set (for the year 2021) with the OECD's DSTRI reveals interesting findings. In Figure 11 we see that perceived AI risks appear to be negatively correlated with the DSTRI. Countries with a higher share of the population who think AI will help over the next 20 years have a lower DTRI index – in other words, these economies are more open to digital trade in services. Similarly, looking in Figure 12 at the share of the population that perceives AI will be a threat in the next 20 years, we see that as the perceived AI risks increase, the DSTRI increases – that is, economies become less open to digital trade in services – although this correlation appears to be weaker.

FIGURE 11. COUNTRY-LEVEL SCATTERPLOT OF PERCEIVED BENEFITS OF AI AND DSTRI

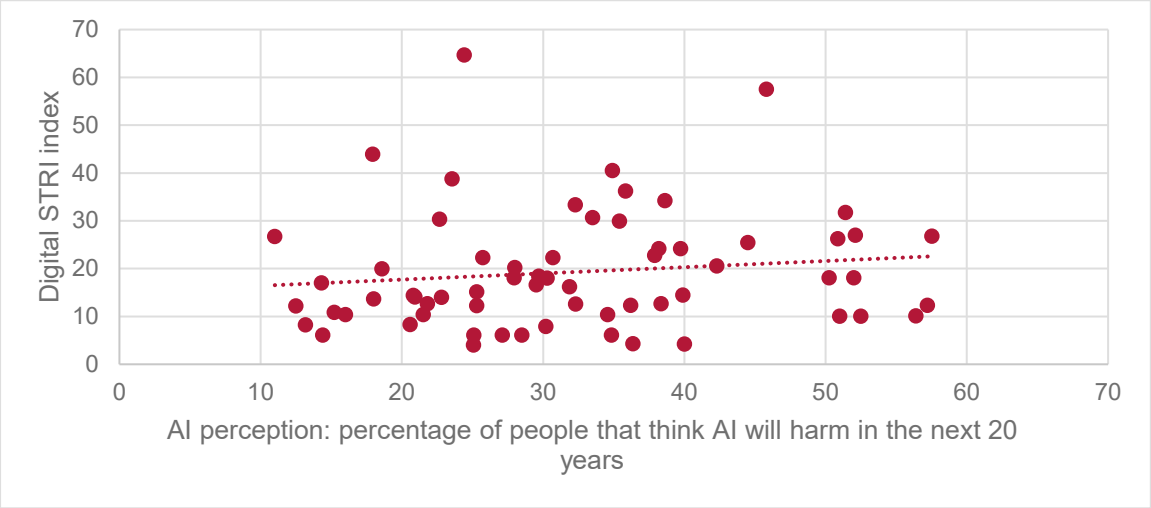


Notes: Scatterplot of country-level risk perception of AI and data privacy (X-axis) from the WRP against country-level information on the DSTRI of 2021 (Y-axis) from the OECD STRI database. The relationship between perceptions of digital risks and digital regulations is likely to be two-way, with one affecting the other. Figure 11 makes no assumptions about causation between the two variables. It shows a negative correlation.

Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

.

FIGURE 12. COUNTRY-LEVEL SCATTERPLOT OF PERCEIVED HARMS OF AI AND DSTRI



Notes: Scatterplot of country-level risk perception of AI and data privacy (X-axis) from the WRP against country-level information on the DSTRI of 2021 (Y-axis) from the OECD STRI database. The relationship between perceptions of digital risks and digital regulations is likely to be two-way, with one affecting the other. Figure 12 makes no assumptions about causation between the two variables. It shows a positive correlation.

Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

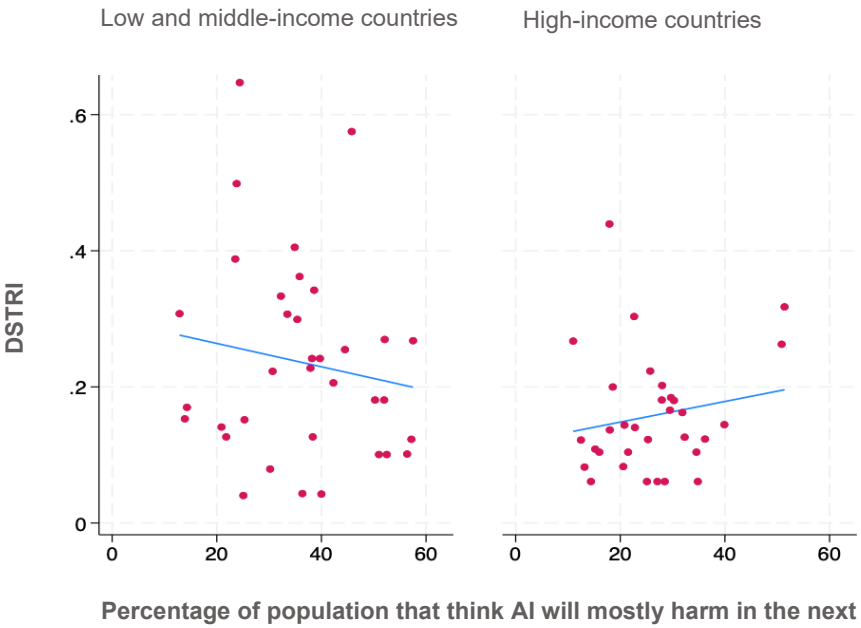
Analysing the relationship across income levels reveals a more nuanced picture (Figure 13). In high-income countries (Figure 13, right), as the share of the population that thinks AI is going to be harmful in the next 20 years increases, the DSTRI increases – in other words, governments restrict digital services trade. However, in the case of LMICs, the opposite correlation is seen; despite increased risks to AI (in terms of perceptions), the DSTRI falls – that is, countries become more open to digital trade (Figure 13, left).

Similar to our findings on data risks, we note that developed and developing countries respond to AI risks differently. In high-income countries, higher AI risks are correlated to a higher DSTRI – in other words, the economies become more closed to digital services trade. But in developing economies, the DSTRI tends to be negatively correlated to AI risks. There are multiple possible explanations for the different relationships for high-income countries and low- and middle-income countries. First, governments in middle- and low-income countries are likely to have less engagement or consultation with the public when designing digital trade policies, while high-income countries are likely to have higher engagement. Developing countries tend to be less democratic in digital policymaking, as evidenced by restrictions of digital rights in Pakistan and Kenya, and the low presence of digital rights advocacy groups in countries like India and Kenya.[65] In contrast, in high-income countries, evidence suggests that digital policies are formulated in more democratic,

[65] Shahab et al. (2023). *Digital authoritarianism and activism for digital rights in Pakistan*. Research Perspectives, Populism and Politics Program, Alfred Deakin Institute; India Development Review (2022). Data protection and digital rights in India; Deutsche Welle (2019). Kenyans must defend their digital rights. *DW Akademie*.

consultative ways. For example, Canada's digital charter and the EU's GDPR were formulated following extensive consultation with stakeholders.[66]

FIGURE 13. DSTRI AND AI RISKS, BY INCOME LEVEL, LMICS (LEFT) AND HICS (RIGHT)



Notes: Scatterplot of country-level risk perception of AI (percentage of population that think AI will mostly harm in the next 20 years on the X-axis) from the WRP against country-level information on DSTRI of 2021 (Y-axis) from the OECD STRI database.

Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; OECD (2025). Digital Services Trade Restrictiveness Index.

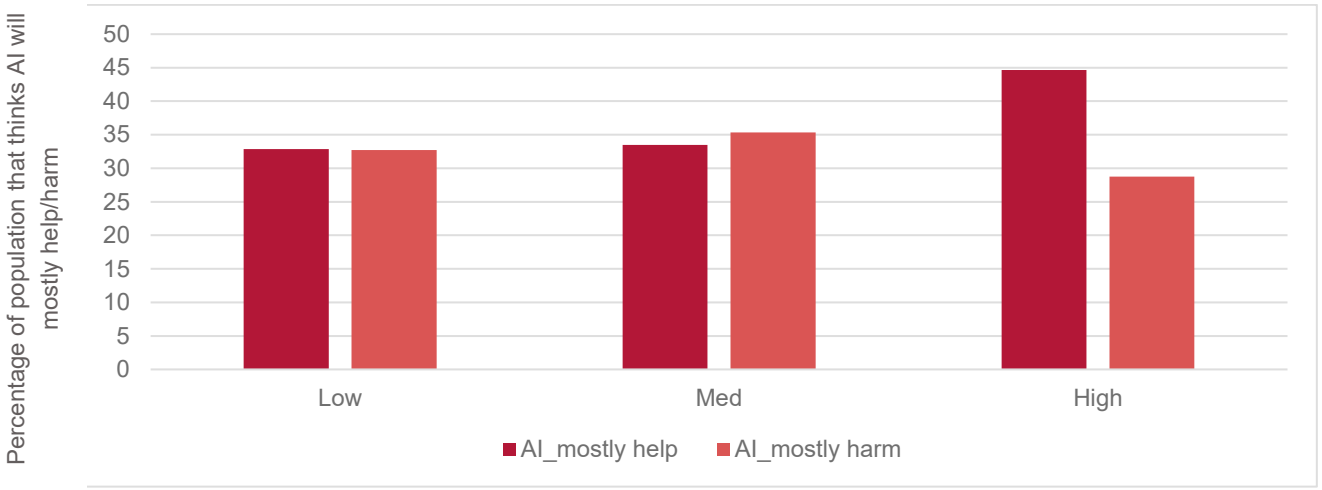
In high-income countries, public concern about AI ethics, privacy, and potential harms may lead to increased political pressure for greater restrictions. Governments may implement more trade restrictions in response to public fears, especially if there is a perception that foreign companies or technologies pose a threat to societal values or security. For example, despite increases in compliance costs for firms,[67] data privacy laws were adopted in the EU in the form of GDPR to address rising concerns about personal data. Similarly, if the population perceives that AI could cause significant harm – whether in terms of job displacement, surveillance, privacy violations, or discrimination – governments may feel compelled to adopt more restrictive policies to protect their citizens. Overall, high-income countries tend to prioritise national security concerns over economic interests in digital trade, in contrast to middle- and low-income countries.

[66] Innovation, Science and Economic Development Canada (2019). Canada's Digital Charter in Action.
[67] McQuinn, A. and Castro, D. (2019). The costs of an unnecessarily stringent federal data privacy law. Information Technology and Innovation Foundation.

6.3 AI risks and digital trade regulation

Figure 14 matches and merges information from TAPED on countries' participation in trade agreements with digital trade provisions and AI risks from Lloyd's WRP. Countries are divided into three quantiles of digital regulatory preparedness – low, medium, and high – based on the number of agreements with a provision on e-commerce/digital trade. Figure 14 shows that in countries with high digital regulatory preparedness, around 45% of the population think AI will help over the next 20 years, compared to less than 35% of the population with medium/low digital preparedness. Similarly, a lower share of the population in countries with high digital preparedness think AI will be harmful over the next 20 years.

FIGURE 14. AI RISKS ACROSS DIGITAL TRADE REGULATORY PREPAREDNESS QUANTILES



Source: Lloyd's Register Foundation (2021). World Risk Poll 2021; and Burri et al. (2022). TAPED data set.

7. Policy recommendations

7.1 Global implications

This brief has highlighted the significance of risk considerations in digital trade and the need to embed a risk-based approach in digital trade agreements regarding AI and cross-border data flows. The Digital Economy Framework Agreement (DEFA) must therefore adequately address data sovereignty requirements and concerns, even as it aims to foster free cross-border flows of data. It would be prudent for there to be exceptions to commitments made by countries to free flows of data, allowing for data flow restrictions based on safeguarding personal data privacy and national security and ensuring ethical use of AI technologies.

Moreover, complexities in cross-border data generation, transfer, and usage, and the risk of cybercrimes, privacy violations, and intellectual property rights infringements associated with artificial intelligence, make it necessary for the DEFA to introduce robust mechanisms for enforcement and dispute resolution concerning cross-border trade in data and AI technologies. Ongoing DEFA negotiations aim to introduce legally binding commitments to address these issues.

Mechanisms for enforcement would potentially involve bilateral collaborations between data protection authorities, an example of which is the MoU between the USA's FTC and the Dutch and Irish DPAs, respectively, and multilateral arrangements to facilitate cross-border cooperation in enforcing data protection and privacy laws, like the Global Cooperation for Privacy Enforcement.[68] Existing dispute resolution mechanisms, such as ASEAN's dispute settlement mechanism, may be upgraded with changes to existing procedures or the addition of new ones that are relevant to the trade in data and AI technologies.

As shown in Sections 5 and 6, perceptions of, and responses to, digital risks vary across countries based on their income and digital integration levels, suggesting that the approach to data and AI governance needs to be flexible and context-specific. Hence, digital policy design in countries should involve consistent engagement and consultation with stakeholders.[69]

7.2 ASEAN-specific implications

As highlighted in this brief, ASEAN Member States have different levels of digital economy development in terms of digital infrastructure, skills, policy frameworks, and markets. This leads to differences in the cross-border digital trade policy prerogatives of digital leaders and digital laggards. The consultations revealed that, unlike the EU, the ASEAN approach (in AI, data protection, and digital trade) is consensus-based and focuses on principles and interoperability,

---

[68] Kastlová, H. (2024). Report on the Extraterritorial Enforcement of the GDPR. Brussels: European Data Protection Board.

[69] Helbig et al. (2015). Stakeholder engagement in policy development: Observations and lessons from international experience. In M. Janssen, M. A. Wimmer and A. Deljoo (eds.), *Policy Practice and Digital Science: Integrating Complex Systems, Social Simulation and Public Administration in Policy Research*. Cham: Springer, pp. 177–204. https://doi.org/10.1007/978-3-319-12784-2_9

primarily due to differences in AI/digital readiness across countries. Guidelines for monitoring, auditing, and accountability in AI systems in the *ASEAN Guide on AI Governance and Ethics* should therefore address the needs and perspectives of AI actors and potential users in ASEAN countries. This makes it prudent to employ context-informed approaches to formulating guidelines, including steps such as landscape assessments and public consultations.[70]

The primary concerns about preserving human rights in AI trade will vary from country to country. For example, the prevalence of the data annotation industry in the Philippines may make the risks of data worker exploitation a higher priority there than consumer data privacy violations.[71] The guide should therefore be holistic, accounting for the different prerogatives of countries.

While the guide addresses concerns about algorithmic biases and the impact of AI on human rights, it does not provide implementation steps for mitigating these risks in the use of AI-based technologies.[72] Providing implementation steps would make the guide more actionable and more impactful in improving AI-related risk cultures.[73] The ASEAN responsible AI roadmap is designed to supplement the guide with a practical implementation tool. Malaysia is also championing the safe deployment of AI through establishing an ASEAN-wide AI safety network (ASEAN AI Safe).[74] This network will facilitate AI safety research, and the development and adoption of responsible AI, and encourage interoperability of AI safety across Member States.

Effective regulation of generative AI trade requires an understanding of data privacy and other ethical concerns in light of the various complexities in the functioning of generative AI, including the constant use of large-scale databases, tokenisation, and bootstrapping of data.[75] Cross-border policies that are less informed about the workings of generative AI technologies may be inefficient in regulating AI and data-related trade, potentially increasing the risk of data privacy violations and international legal disputes. Hence, it is important for trade agreements to involve collaborations between countries on understanding AI-related developments and ethical concerns, to improve and evolve the terms of their agreements. The Singapore–UK DEA, which seeks cooperation between the countries on issues and developments relating to AI, including the "ethical use, human diversity and unintended biases, industry-led technical standards and algorithmic transparency", could be a useful starting point for ASEAN Member States' future trade agreements. [76]

---

[70] Nørbech, I. (2023). Does policy context matter for citizen engagement in policymaking? Evidence from the European Commission's public consultation regime. *European Union Politics*, 25(1), pp. 130–150.
[71] Simon, T. (2024). Navigating the AI revolution, *HesaMag*, 29 (Winter 2024). Available at: https://www.etui.org/publications/navigating-ai-revolution (Accessed: 15 January 2025).
[72] *ASEAN Guide on AI Governance and Ethics* (ASEAN 2024).
[73] *ASEAN Guide on AI Governance and Ethics* (ASEAN 2024).
[74] Ministry of Digital, Malaysia (2025).
[75] Gualdi, F. and Cordella, A. (2024). Theorizing the regulation of generative AI: lessons learned from Italy's ban on ChatGPT.
[76] UK–Singapore Digital Economy Agreement, 2022.

Appendix A. Consultation participants

- Dr Agusta Samodra Putra, Researcher, Centre for Sustainable Production System and Life Cycle Assessment, National Research and Innovation Agency (BRIN), Indonesia
- Dr Bernard Leong, CEO, Dorje AI and Adjunct Associate Professor, NUS Business School
- Dr Dedy Permadi, Chairman of the National Taskforce for AI Talent Development, Coordinating Ministry for Human Development and Cultural Affairs, Indonesia
- Representative, Executive Director, Institute for Development of Economics and Finance (INDEF)
- Dr Lili Yan Ing, Lead Advisor (Southeast Asia), Economic Research Institute for ASEAN and East Asia (ERIA)
- Dr Maria Monica Wihardja, Visiting Fellow and Co-coordinator of the Media, Technology and Society Programme, ISEAS-Yusof Ishak Institute
- Dr Nopparuj Chindasombatcharoen, Research Fellow, Industrial Policy, Thailand Development Research Institute (TDRI)
- Dr Sophal Try, Director-General, General Department of Science, Technology and Innovation, Ministry of Industry, Science, Technology and Innovation, Cambodia
- Dr Taojun Xie, Lecturer, Nanyang Technological University
- Mr Clemence Tan, Partner, Cybersecurity and AI Risk Management, Artificial Intelligence International Institute (AIII)
- Mr Darren Grayson Chng, Regional Data Protection Director, Electrolux Group
- Mr Ferro Ferizka Arnayananda, Senior Advisor to The Coordinating Minister, Coordinating Ministry for Human Development and Cultural Affairs
- Mr Hazremi Hamid, Senior Officer, Digital Economy Division, ASEAN Secretariat
- Mr Ray Frederick Djajadinata, Technology Partner, Alpha JWC Ventures
- Mr Thomas Tilley, Digital Economy and Technology Lead, APAC, Department Business and Trade
- Mr Yeong Zee Kin, Chief Executive, Singapore Academy of Law
- Mr Yudanto Wibowo, First Secretary, Permanent Mission of the Republic of Indonesia to the UN, WTO, and other international organisations
- Ms Kristina Fong, Lead Researcher (Economic Affairs) at the ASEAN Studies Centre, ISEAS-Yusof Ishak Institute
- Representative, Institute for the Public Understanding of Risk, National University of Singapore
- Professor Mohan Kankanhalli, Director, NUS AI Institute

Policymaking for a more resilient world

The project *Policymaking for a more resilient world: leveraging the World Risk Poll for more effective digital, labour, and industrial policies* is led by Cambridge Industrial Innovation Policy, in partnership with UNIDO, and funded by Lloyd's Register Foundation. It draws on the Lloyd's Register Foundation World Risk Poll and interconnected data sets to examine perspectives on AI, digital, labour, and industrial policy, focusing on the Southeast Asia region. The project aims to inform policies that ensure a safer and more sustainable future for all.

Cambridge Industrial Innovation Policy

Cambridge Industrial Innovation Policy (CIIP) is a global, not-for-profit policy group based at the Institute for Manufacturing (IfM), University of Cambridge. CIIP works with governments and global organisations to promote industrial competitiveness and technological innovation. We offer new evidence, insights and tools based on the latest academic thinking and international best practices.

This report was delivered through IfM Engage, the knowledge-transfer arm of the Institute for Manufacturing (IfM), University of Cambridge.

Cambridge Industrial Innovation Policy, 17 Charles Babbage Road, Cambridge, CB3 0FS, United Kingdom

WWW.CIIP.GROUP.CAM.AC.UK