Tallinn Digital Summit

digitalsummit.ee

Briefing note: AI & Trade Policy

By Hosuk Lee-Makiyama — Director of European Centre for International Political Economy

Summary:

Businesses use artificial intelligence to optimise their products, serve customers and better understand overseas markets. Commercial use of A.I. anticipates access to data abroad in an orderly manner. Access to market data is essential for manufacturing competitiveness and the ability to serve export markets.

How can trade policy support A.I development and avoid being stuck in a defensive rut?

The future ability to export is pending on AI: how much we can learn, or process data, about overseas markets

Introduction: Trade rules matter for AI.

As we are two centuries into the digital age, it is self-evident that the use of data is essential for a range of commercial activities, and in all industrial sectors. Moving data across different markets are central to conducting cross-border transactions.

There is substantial economic value involved, especially for major exporters such as the EU. Services exports depending on the internet bring 495 billion annually in export revenues, without which the EU would enter into a severe balance of payment deficit.

Artificial intelligence takes the industrial digitalisation even further. Machine and deep learning also change how traditional industries and SMEs compete overseas. For instance, predictive analysis brings down costs and risks in emerging markets. Natural language processing allows a family business in France to service thousands of customers in dozens of languages from their home office.

AI minimises physical and cultural distances or barriers at a very low cost. Still, a number of regulatory measures impede on its evolution. Forced or coerced *localisation* of data is now widely in practice. Personal data is increasingly restricted from being transferred out of a jurisdiction. Some jurisdictions require *disclosure of commercial source codes* including algorithms. Without adequate copyright safeguards, algorithms can be barred from reading and processing what's openly available on the internet.

IT-systems, servers and customer management make up a considerable share of business costs. Duplicating them on every overseas market makes exporting commercially unviable for SMEs and multinationals alike. However, there are divergent of views amongst the global powers on how such barriers should be addressed.

Disciplines that limits such requirements to necessary and justified situations feature in trade agreements, including the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) and the recently published US-Mexico-Canada (USMCA) agreement. In contrast, the EU and China take a cautious rut, despite being the world's largest and second largest exporters respectively. Insights from AI bring competitive advantage in the global industrial competition – just like better market knowledge, branding or efficient production chains. The future ability to export is pending on AI: how much we can learn about overseas markets through processing data.

Data matter for AI innovation, exports and national accounts

Market assessments estimate the value of all commercial transactions conducted between consumers (B2C), business (B2B) and peer to peer (C2C) to US$ 2.3 trillion in 2017, and still growing at 25% per year.[1] In other words, if e-commerce was a sovereign economy, it would be of the equivalent size of India or Russia, and still grow four times faster than the Chinese economy,[2] and the world would be lining up to sign trade agreements with it.

However, the true value of the data-driven commerce exceeds just sales of goods and services via the internet. Firstly, the internet has not just allowed more services to be tradable across borders, but cross-border data flows have effectively become the "carrier

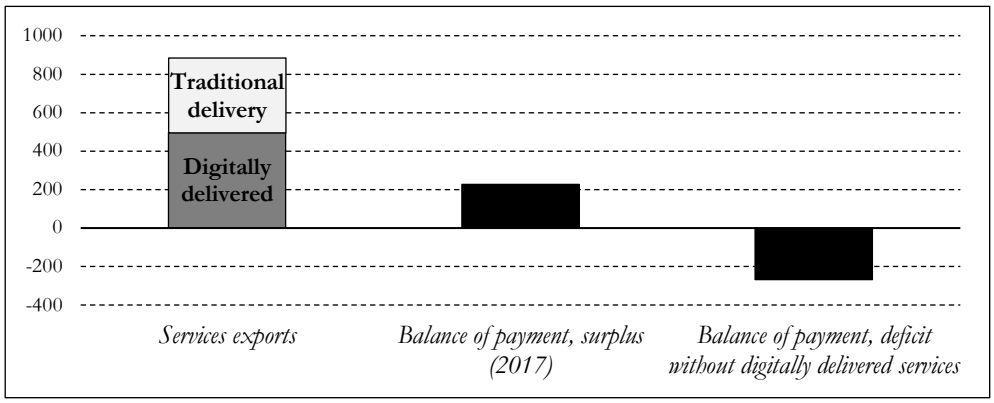
[1] eMarketer, *Worldwide Retail and Ecommerce Sales*, 2018

[2] World Bank, *World Development Index*, 2016

wave" of trade in services, and the dominant mode by which services are traded cross-border ('mode 1' and 'mode 2' in trade law parlance). Trade economists estimate that 56% of EU services exports (or 495 billion euros) in retailing, banking, professional or engineering services are enabled by and depending on connectivity.[3] The EU would enter into a severe balance of payment deficit without these revenues (figure 1), which are 3.5 times larger than the motor vehicle exports – Europe's largest export industry.[4]

Figure 1 — EU enters into a balance of payment deficit without digitally supported service

The EU enters into a severe balance of payment deficit without the surplus from digitally delivered services.



Source: author's calculations based on Eurostat, 2018; Nicholson, 2017

Secondly, cross-border data flows are an essential input for business processes and innovation. Deep or machine learning (DL and ML) depend on access to observations, such as user behaviour to train models to recommend decisions or make predictive analyses. Empirical studies have measured the data usages of various industrial sectors (figure 2),[5] that even exceeds the average net profit margins of the sectors.[6] In other words, government regulations that result in rises in software and data costs could effectively prohibit market entry.[7]

[3] Nicholson, J., *ICT-Enabled Services Trade in the European Union*, US Department of Commerce, ESA Issues brief, 3-2016.

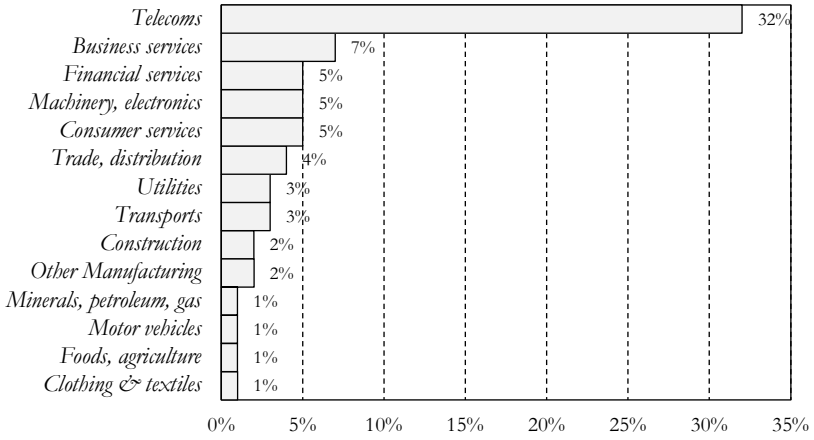
[4] Eurostat, 2017

[5] Bauer, Lee-Makiyama, van der Marel, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE, 2014; based on US Bureau of Economic Analysis, Input & Output Account Data, 2007

[6] See gross operating profits under Foreign Affiliates Statistics of US BEA, 2017 and Eurostat, 2016

[7] *ibid.*

Figure 2 — Importance (by value) of data, software and connectivity in production



Source: Lee-Makiyama, Bauer, van der Marel, 2014

Building AI on personal information

Needless to say, the 'digital' share of the economy is expected to grow – and the use of personal information fuel that growth: Understanding natural speech, text or identifying people and object require access to recordings and transcripts. Observations on user and customer behaviour is *de facto* such data, while the vast majority of all transfers (approx. 75% of all transmitted data) was user-generated by 2012.[8]

In addition, even non-personal information in the form of enterprise and operational data (e.g. technical readings of machinery, or stock inventory) stored within a corporate network contains information on personnel who are logged in while collecting or analysing data. Also, *metadata* – such as phone numbers, email or IP addresses – and is contained within all online communication. They may not reveal personal identity *per se* but still could make users identifiable, why some jurisdictions equal them to personal information.

A malevolent regulator could use personal data protection laws to block any data transfer between two points and stop trade.

Personal data ingrained in data transfers make them *mixed data sets* of personal and non-personal data that are technically and legally inseparable. Such sets have been discussed in the context of intra-EU free flow of data in Europe, which aimed at liberalising only *non-personal* data.[9] This fact has a major implication on trade: In effect, a malevolent regulator could use personal data protection laws to block *any* data transfer between two points and stop trade.

In the meanwhile, the number of restrictive measures on cross-border transfer is on the rise. Number of restrictions have quadrupled since the millennium, doubled since smart devices were introduced in the last decade (figure 3a). The majority of these measures are applied horizontally across all industrial sectors for all sectors (figure 3b).[10]

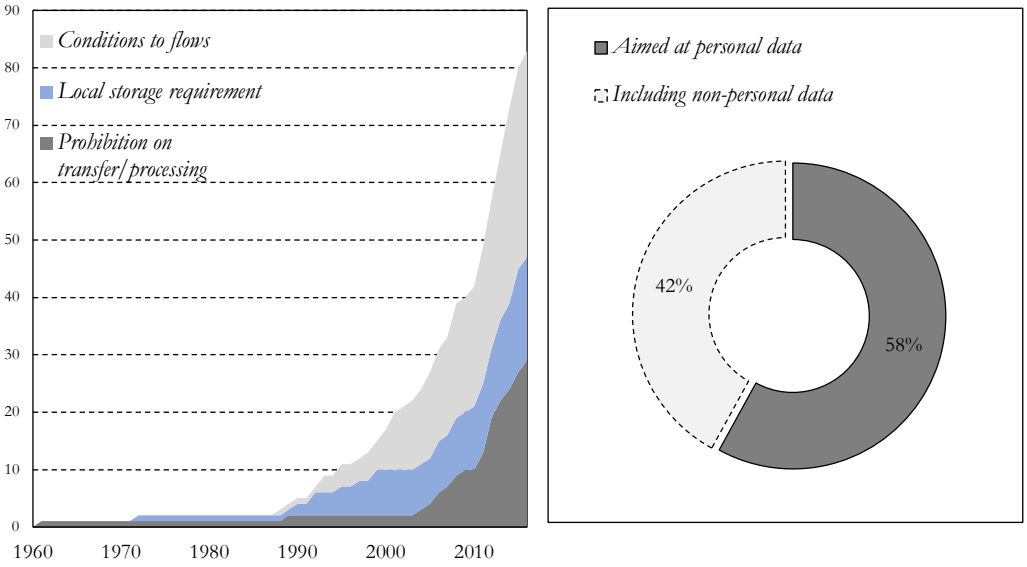
[8] Tucker, P., *Has Big Data Made Anonymity Impossible?*, MIT Technology Review, May 2013

[9] Bulgarian Presidency of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union – Examination of the Presidency text,* Brussels, December 5, 2017, accessed at: http://data.consilium.europa.eu/doc/document/ST-15112-2017-INIT/en/pdf

[10] ECIPE, *Digital Trade Estimates*, 2018

The majority of data localisation measures in the world are pursued for privacy objectives – for all sectors, not just for platforms.

Figure 3a/b — data localisation measures and conditions to cross-border data flows imposed in 65 economies



Source: Ferracane, Lee-Makiyama, van der Marel, Digital Trade Estimates, 2018

Meanwhile, some governments seize algorithms.

Grossly simplified, algorithms are schematics of rules that are used for problem-solving. In real life, algorithms are implemented and supplied as lines of code in software or an online service. As such, AI algorithms are not typically protected as intellectual property (which must be publicly shared to be protected), but fit into another category of assets, namely *trade secrets*.

Trade secrets (or confidential information) could be formulas, recipes, the names of clients or production processes, that remain unpublished and instrumental to any knowledge-intensive sector. However, some legal systems do not acknowledge the concept of trade secrets or protect source codes or algorithms.[11] Other jurisdictions explicitly demand algorithms and source codes to be shared with the public authorities.[12] But there are no obvious reasons why countries, who do not require food producers to surrender their secret recipes despite their impact on public health,[13] would ask businesses to share their algorithms *ex ante*, before they are suspected of causing immediate harm.

There is no obvious reason why the authorities should misappropriate all algorithms when they don't ask for recipes of food producers

In particular, the context of public procurement and government purchase of software and e-government solutions provide an occasion where private firms may be coerced to surrender source codes and reveal their competitive advantages. Discrimination in public procurement can be a commercial impediment in its own right, as it could cover up to 15

[11] According to the original Turkish doctrine, trade secrets and IPRs are incompatible; see comments by AIPPI, *Protection of trade secrets through IPR and unfair competition law*, accessed at: https://www.aippi.org/download/commitees/215/GR215turkey.pdf

[12] Russian Federal Security Services also demand internet companies to hand over any encryption keys. Failure to comply lead to their services being blocked in Russia in accordance with the 2016 *Federal Law No. 374 on Amending the Federal Law on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety*.

[13] Government of India demanded that the secret to recipe for Coca Cola in 1977; Coca Cola Company, *Who knows the secret formula of Coca-Cola*, accessed at: https://www.coca-cola.co.uk/faq/who-knows-the-secret-formula-of-coca-cola;

per cent of GDP of some countries and ruin the commercial viability of the entire market.[14] Also, regulators could pass on source code or proprietary algorithms to their competitors or a state-owned enterprise.[15] Procurement laws of India, Colombia, Indonesia and China allow the governments to misappropriate commercial algorithms and source codes.

While there are strong national security and defence objectives to retain that right, they may not be exercised proportionately. For example, China routinely designates any IT system used within its public sector (including its many state-owned enterprises) as *critical infrastructure* (CI).[16] Russia examines business and anti-virus software on national security grounds, which at first sight may seem reasonable. However, the source code review allows Russia to find exploitable vulnerabilities in products that are widely used by other governments.[17]

Why is it illegal for algorithms to read what humans can read online for free?

Finally, other ideas have a bearing on the adaptation of AI technologies – most of them springs from Europe. *Text and data-based mining* (TDM) techniques involve algorithms scanning through publicly available texts and images online to learn how to interpret languages,[18] or to teach autonomously driving software to distinguish road signs or people from other obstacles.[19] Some legislators have proposed banning commercial enterprises from engaging in TDM,[20] while stopping algorithms from reading what is publicly available online (that humans can read free of charge),[21] limits the notion of 'fair use' or 'fair dealing' of copyright protected materials.

Who should be liable if algorithms fail?

With every prototype using AI and autonomous decision-making, there is a growing ethical and legal discussion on the *liability* arising from failing algorithms and the damage they cause. The typical question involves the extent an AI developer is liable if a self-driving vehicle causes an accident; or if a credit-approval algorithm starts to discriminate certain minorities? These questions are not just legal but also ethical dilemmas.

Autonomous driving may save tens of thousands of lives per year lost in traffic accidents, while doctors using AI to assist in diagnostics and treatment plans may save even more lives. But for these market to actually emerge, the liability for the AI developers must be well-defined and proportionate.

AI-assisted diagnostics may save tens of thousands of lives. But for these markets to emerge, the liability for AI developers must be proportionate

The question of the legal liability for AI usage is already ongoing in criminal and tort law,[22] spawning some divergent views. A few legislators have even gone as far as

[14] Ferracane, Lee-Makiyama, *China's Technology Protectionism and Its Non-negotiable Rationales*, ECIPE, 2018

[15] IBM, *Comments of IBM Corporation in Response to Federal Register Docket # 82 FR 29622 – "Request for Comments Regarding the Administration's Reviews and Report to the President on Trade Agreement Violations and Abuses",* 2017

[16] *ibid.*

[17] U.S. Department of Defense, Letter in response to Senator Jeanne Shaheen, December 7, 2017, accessed at: http://fingfx.thomsonreuters.com/gfx/rngs/USA-CYBER-RUSSIA/010060650E4/Shaheen_HPE%20Source%20Code_7%20Dec%20(DoD%20CIO%20signed(.pdf

[18] OpenMinted, *How Zalando links languages with TDM*, accessed at: http://openminted.eu/tdm-stories-zalando-links-languages-tdm/

[19] European Commission, *Data Mining Knowledge and technology flows in priority domains within the private sector and between the public and private sectors*, February 2017

[20] European Commission, *Impact Assessment on the modernisation of EU copyright rules*, SWD/2016/0301 final, 2016/0284

[21] European Parliament, *The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market - Legal Aspects*, JURI, February 2018

[22] Kingston, J., *Artificial Intelligence and Legal Liability*, February 2018,

suggesting establishing personhood for robots (that are merely AI applications in physical casings),[23] making the algorithms themselves accountable when they fail, rather than the norm of holding the manufacturer their users accountable by *culpa in eligendo* – the negligence by choosing wrong tools.

A third principle holds the inventor accountable rather than the user. Under a so-called *innovation principle*, a developer has strict liability for its products, regardless by whom or how the product is used. As a comparison, would carmakers of the past be held liable for traffic accidents – while exonerating intoxicated or reckless car drivers? It is hard to see why AI would be subjected to harder or different product liability than medical devices, traditional cars or consultants in general.

Which countries will be the most AI-restrictive?

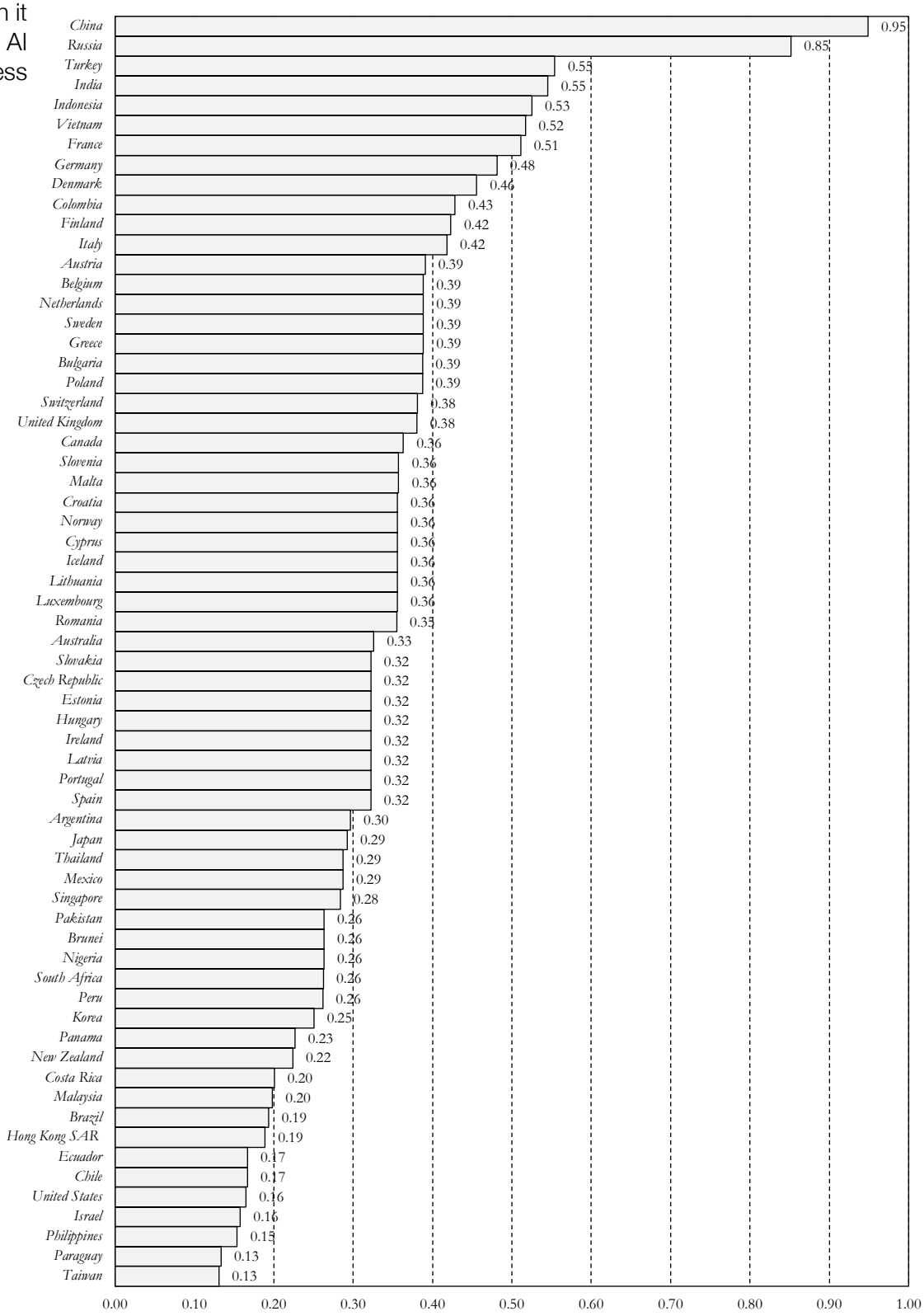
Recent applied research in economics shows that future regulations that impede on the deployment of AI will inhibit the productivity of the economy – and there is also a link between a country's ability to export and how much data it can access or process.[24]

A non-weighted score of trade restrictiveness applied for these measures on source codes, fair use or dealing online, cross-border data flows and proportionality in data use reveal a considerable divergence in the world (figure 4). Those countries who tend to be restrictive or disproportionate in their governance of the digital economy tend to be so consistently across all policy areas – i.e. countries such as China and Russia place themselves in a category on their own, while EU and OECD countries are concentrated in the middle tier. The least restrictive economies are a mixed group of global innovation leaders in software development as well as jurisdictions that are 'regulatory greenfields' – a group of countries that are yet to enact relevant privacy regulations – which does not make their economic policies more AI friendly. Indices of regulatory restrictions are namely just that, a measure on whether regulations restrict technologies, and not necessarily a measure whether the policy environment encourages or promotes them.

[23] European Parliament, *Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103 INL)
[24] *Supra* note 5.

China and Russia are in a category of their own when it comes to AI restrictiveness

Figure 4 – Trade restrictiveness for AI (based on lack of protection of algorithms, mandatory source code disclosure, limitations on TDM, fair use/dealing, conditions on cross-border data flow or data localisation, disproportionate administrative burden or sanctions)



While trade agreements typically cut tariffs collected at the border or remove investments of farm produce quotas, they typically do not rewrite national laws assessed in this AI restrictiveness index. Trade agreements do not directly *regulate* issues like privacy, data flows or IPRs: The treaties do not specify what the rights of citizens or corporations should be, but merely stop consenting governments from worst forms of discrimination or inadequate standards.

Recent trade agreements, starting with the Trans-Pacific Partnership (TPP) – originally signed by the US, Japan and ten other Asian-Pacific economies in 2016 –[25] set a new benchmark on digital trade for its members. The TPP chapter on digital trade is one of the very few chapters that remained unchanged and unabridged when the remaining countries redacted and renamed it into the Comprehensive and Progressive TPP (CPTPP) after the US withdrawal.[26]

The CPTPP rules update the universal WTO rulebook, that removed discrimination on voice-over-IP calls, online gambling, online entertainment and payments,[27] by reinterpreting agreements that predates the internet.[28] Meanwhile, new agreements since CPTPP offer a rulebook with more specificity. Rules on data flows deals with *data flows* explicitly– and not through extrapolation of *public telecommunications transport networks*.[29]

In addition, the new agreement between the United States, Mexico and Canada (USMCA) on October 1st, 2018, amending the NAFTA agreement contains new provisions with particular relevance to AI.

The benchmark on digital trade rules: CPTPP

CPTPP protects cross-border data flows and bans data localisation measures unless for 'legitimate policy objectives' that are proportionate.

Cross-border data flows and data localisation

The CPTPP chapter on e-commerce affirms the general principle thatthe free choice of apps and services on the internet ultimately benefits consumers.[30] It updates the existing WTO rules by protecting data flows, and data localisation measures as barriers. The parties *shall allow* for "cross-border transfer of information by electronic means."[31] In addition, CPTPP bans its parties from imposing data localisation requirements that "require a covered person to use or locate computing facilities in that Party's territory".[32]

This pair of provisions exempts domestic regulations that serve a *legitimate public policy objective*, given that the restrictions pass a two-tier test through *legitimacy* (no "arbitrary or unjustifiable discrimination", or "disguised restriction"),[33] and *proportionality* (not "greater than are required to achieve the objective").[34]

Such exceptions correspond to the catalogue of cases for exceptions (albeit with slightly different wordings) under WTO rules granted for a limited set of objectives than CPTPP's unspecific exemption for any legitimate objective,[35] while the CPTPP also

[25] The original TPP agreement between the governments of Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam, and United States signed on 4 February 2016.

[26] Agreed amongst all parties except the United States on 8 March 2018.

[27] United States—*Online Gambling*, DS285; Mexico—Telmex, DS204: Telmex, China—*Audiovisual Entertainment Products*, DS363; China—*Electronic Payment Services*, DS413

[28] WTO General Agreement on Trade in Services,

[29] Term used within WTO GATS Annex on Telecommunication, 1996

[30] CPTPP 14.10; USMCA 19.10

[31] CPTPP, 14.11

[32] CPTPP, 14.13

[33] CPTPP, 14.11 para a which paraphrases the WTO two-tier test under GATS article 14 and GATT article 21

[34] *ibid.*

[35] GATS, art 14. For a legal discussion on WTO exceptions and the digital economy, see Hindley, Lee-Makiyama, *Protectionism Online*, ECIPE, 2009

exempts the entire financial industry from these provisions.[36] Carve-outs under the CPTPP are still as wide (if not wider) than before under WTO rules – and to prove the case in point, Vietnam amended its data localisation requirements in June 2018 by invoking national security objectives,[37] despite its intention to ratify the CPTPP.

Protection of source code

CPTPP protects against appropriation of source codes, but only for mass-market products, not used on critical infrastructure.

Similar to the provisions against data flow restrictions, CPTPP explicitly prohibits mandatory source code disclosure by governments. Prior to the FTAs, the universal rules under the WTO merely require governments to protect commercial trade secrets without explicitly covering software or algorithms.[38]

CPTPP article 14.17 states that "no party shall require the transfer of source code", but only for *mass-market* software that is not used for *critical infrastructure*.[39] By explicitly dealing with *source code* (rather than trade secrets or software patents), CPTPP protects developers' code whether it qualifies as an IPR. A line of code used in a software is always source code whether it qualifies as a software patent or not, which governments may not appropriate without justifications.

However, CPTPP limitation to *mass-market* software disqualifies most AI applications today in the business segment. *Critical infrastructure* exclusion applies to a large section of the AI customer base, including transport, telecom and financial sectors, or public administration.[40] As CPTPP explicitly protects code for *software*, some may argue that an AI algorithm used for an online *service* (say, AI-driven predictive keywords on a search engine; or an online store using AI-based recommendations or personalisation) falls outside that definition.

The new USMCA (NAFTA) agreement addresses some AI-specific issues

Cross-border data flows and data localisation

While CPTPP sets a new benchmark for what trade agreements can do for openness and non-discrimination on data flows, the new USMCA agreement further strengthens and clarifies the commitments for the United States, Mexico and Canada.

Firstly, USMCA clarifies the level of protection that the parties must achieve on the protection of personal information. The USMCA references international guidelines,[41] and legislative concepts that should be considered in the domestic privacy legislation –[42] whereas the CPTPP agreement only prescribed there must be a legal framework for

[36] Definitions under CPTPP 14.1

[37] Government of Vietnam, *Law 24 on Cybersecurity*, 12 June 2018, English translation accessed at: https://www.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf; see also Nikkei Asia Review, *Vietnam's cybersecurity law sparks concerns from businesses, June 12, 2018*, accessed at: https://asia.nikkei.com/Politics/Vietnam-s-cybersecurity-law-sparks-concerns-from-businesses

[38] WTO, TRIPS, article 39

[39] CPTPP, 14.17 para 1 & 2

[40] The definition of critical infrastructure is different in in each jurisdiction

[41] USMCA, 19.8.2

[42] USMCA, 19.8.3 mentions limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.

protecting personal data in place,[43] without specifying the level of protection,[44] which is "non-discriminatory".[45]

Secondly, the USMCA strengthens the position of AI developers through a simple change of semantics. Where CPTPP states parties "shall allow" transfer of information, USMCA states no party "shall prohibit or restrict" such flows. Thus, mere *restrictions* (e.g. governments slowing down or complicating access to data) are now also within scope, not just outright *prohibitions*. To prove that the governments have failed to *allow* data flows under the CPTPP is also more onerous than to prove a government maintains a *prohibition* – since the existence of the ban is an evidence of treaty breach in itself.

USMCA limits the exceptions on data flow and localisation under CPTPP and protects algorithms against misappropriation

Thirdly, the USMCA removes the exceptions for legitimate policy objections for data localisation – in other words, there may be legitimate reasons to limit data flowing in and out of a country (including privacy protection), but no justifications to force businesses to use local servers and staff to conduct business in a country.

Once again, semantics matter in international treaties: If data cannot flow, then surely that data must be confined and localised in that country? The new USMCA rids countries of storage requirement that allows data to be taken out if a duplicate set of servers stores the data within the country, as applied by countries like Russia.[46] Such practices are already inconsistent with international treaties that prohibit *performance requirements* that force firms to invest to conduct business in a country.[47]

Specific protection of algorithms

USMCA remedies several uncertainties on source codes in the CPTPP text. It amends the scope with *algorithms* in addition to just *software*.[48] USMCA also removes the CPTPP limitations for non-*mass market* products or *critical infrastructure*. Instead, USMCA allows regulatory bodies to engage in "specific investigations, examination enforcement action or judicial proceedings." In other words, governments may scrutinise code to enforce its rules – but not to steal code.

In conclusion, USMCA rules offer more comprehensive protection than CPTPP with fewer exclusions – regardless whether the algorithm is used in a customised business solution or a simple app for mass markets, or whether it qualifies as an IPR or not.[49]

Other relevant provisions relevant to AI development

No jurisdiction may have yet imposed strict liability for AI developers, making them liable for improper use of their products. Nonetheless, the USMCA agreement pre-empts some of the future problems by binding its signatories to limit the liability for *interactive computer services*,[50] which may be drafted with various online platforms in mind. However, Cloud AI services and AI as a service (AIaaS) would fall under its definitions. The liability for harm for such services is limited to the extent the supplier has created or developed the information, precluding future imposition of any stricter form of liability.

[43] CPTPP, 14.8

[44] Footnote to CPTPP 14.8.2 exemplifies the full range of techniques, from comprehensive economy-wide legislation to "voluntary undertakings"

[45] CPTPP, 14.8.3

[46] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation; see also Bauer, Lee-Makiyama, van der Marel, Verschelde, *Data Localisation in Russia: A Self-imposed Sanction*, ECIPE, 2015

[47] See a discussion on performance requirements under US model BIT article 8; also Houde, Yannaca-*Small, Relationships between International Investment Agreements*, OECD Working Papers on International Investment, 2004/01

[48] USMCA, 19.16.2

[49] *ibid,* at footnote.

[50] USMCA, 19.17

Besides the binding rules, USMCA also expresses the shared principles and endeavours of its signatories that may be non-binding – but nonetheless relevant to the deployment of AI in the society. The signatories of USMCA recognises that facilitating public access to government information fosters "economic and social development, competitiveness, and innovation,"[51] and when data is made available, it should be in open machine-readable formats that are suited for AI development.

EU's cautious approach to trade rules

Trade rules can supplement privacy rules

The scores for AI trade restrictions amongst the EU countries vary between 0.31 to 0.51, within a narrower divergence than a heterogeneous group of countries like the CPTPP (that ranges between 0.17 for Chile, and 0.52 for Vietnam). Moreover, the EU Member States share a common set of key regulations that are highly relevant to AI, like the General Data Protection Regulation (GDPR).[52] Many national laws are also based on EU directives, like on IPRs.[53] In fact, the variations in AI restrictiveness is mostly explained by case law, enforcement or issues that outside EU cooperation, e.g. national security.

In the context of digitalisation, GDPR is perhaps the most important political deliverable of the EU in recent years. Trade, and other policy areas, are subject to the limitations and precedence set by EU data protection rules. To begin, the applicability of GDPR is not territorially limited to Europe and explicitly forbids transfers of personal information of EU citizens out of Europe.

GDPR and adequacy decisions determine the right to take personal data *out* of the EU – not the right of EU exporters to use AI analytics in another country

However, there are several reasonable alternatives to transfer personal information out of Europe. Firstly, it is still possible to collect and transfer data with explicit consent from the users. Secondly, some jurisdictions have been formally deemed to have 'adequate protection', although these countries only account for just 16% of EU exports.[54] Businesses can also use certain legal instruments (e.g. binding corporate rules or model contracts), although the developing countries have argued the method to be too time-consuming or too costly to implement.[55]

Europe's approach to data has some limitations for its commercial interests. To begin, adequacy under privacy rules are not bilateral treaties but unilateral decisions taken by the EU alone to allow data to flow to *another* jurisdiction. In other words, adequacy is a one-way street that takes data *out* of Europe, but they are not tools that allow European businesses to take data from another country *into* Europe, to be processed and analysed at their headquarters.

Without its trade policy and by its privacy rule alone, the EU cannot accommodate its commercial interest to use AI to better understand and serve foreign markets, unless it is one of the few countries which does not restrict data. Alternatively, a country must reciprocate Europe's adequacy decision into a two-way street arrangement, like in the case of Japan.[56] Also, privacy rules and adequacy decisions cannot protect EU exporters

[51] USMCA 19.18

[52] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[53] Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15. 6. 2016

[54] All adequacy countries (including Japan), Eurostat, 2017

[55] UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, UNCTAD, 2016

[56] Japan, *Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information*, 2016; also *Enforcement Rules for the Act on the Protection of Personal Information*, 2016

against localisation requirements of non-personal information. As illustrated in figure 3b, many data localisation measures include non-personal information covering all data within a business sector, e.g. the healthcare or financial sectors, or localisation of a certain type of data, like company and tax records.

Cross-border data flows and data localisation

At the time of writing, none of the EU FTAs that are in force includes explicit disciplines on data flows outside of financial services.[57] The latest negotiated agreement, the EU–Japan Economic Partnership Agreement of 2017 (completed a full year after the official announcement of the TPP agreement) resulted in a *rendez-vous* clause, where the parties "shall reassess the need for inclusion of an article on the free flow of data within three years".[58] Uncertainties about how privacy and how it counteracts with trade commitments stuck Europe in a cautious rut.

Since the conclusion of the EU-Japan EPA, the EU has also drafted its new model text for its future trade agreements that is firmly grounded in its philosophy that privacy is a fundamental right,[59] and the laws to safeguard this right is an absolute sovereign prerogative.[60]

New EU trade texts exempt any data localisation measure claimed to be taken for privacy reasons

The EU texts bind the EU and its prospective partners to a high standard equivalent to CPTPP or USMCA for data flows – only to carve out much wider exceptions than the two. The new model text prohibits requirements to use or locate computing facilities,[61] or making data transfers contingent upon use or localisation that address the local storage requirement.[62] The scope actually goes further than CPTPP and USMCA by covering also *network elements*,[63] e.g. not just servers but also when AI becomes integrated with 5G networks and internet of things.[64]

However, the subsequent article voids any commitments in regard to many measure "it deems appropriate",[65] for protection of personal data and privacy without any justifications or conditions.

The EU wordings are carefully chosen. To begin, there are only a few such unconditional exceptions in trade law, reserved for essential national security issues that are existential threats,[66] e.g. arms, nuclear materials and in times of war. The EU texts add privacy to such grave threats.

Secondly, the EU exceptions for privacy covers what "it deems appropriate", i.e. means it is a subjective assessment based on whatever the defendant claims, rather than an objective and plausible one, in the case of a dispute. It is possible to justify any measure, regardless of whether they are reasonable, proportionate or legitimate. To take an example from the past – in 1973, Sweden subjectively deemed its import restrictions on running shoes a national security issue because the armed forces wore them during physical exercises.[67] In conclusion, Europe's counterparts can argue any restrict the use of

[57] EU-Korea FTA, Article 7.43, which is lifted from Korea-US FTA, Chapter 13 Annex 13-B Section B

[58] EU-Japan EPA, Trade in Services, Investments and E-Commerce: 8.81

[59] European Commission, *Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)*, January 2018, article B1

[60] *ibid.,* article B2

[61] *ibid.,* article A1(i)

[62] *ibid.,* A1(iv)

[63] *ibid.*, A1(i)

[64] Li, Zhao, Zhou, Ding, Chen, Wang, Zhang, *Intelligent 5G: When Cellular Networks Meet Artificial Intelligence,* IEEE, 2017

[65] *supra* note 59, article B2

[66] WTO, GATT art XX; GATS art XIV bis

[67] According to the oral records of the Ministry of Foreign Affairs of Sweden, the delegates of GATT (predecessor of the WTO) chose to attend the meetings barefoot to ensure the Swedish counterparts that they come unarmed.

AI (or running shoes) uncontested and even in bad faith, by invoking the proposed privacy exceptions.

Protection of algorithms

The most recent EU trade agreements with third countries contain a limitation on transfer of, or access to, source code of software.[68] Although the language is yet to incorporate algorithms like the USMCA, the EU FTAs include all software (and not just mass market products), with just some exceptions for "voluntary" transfer of code in the context of public procurement,[69] or it may be deemed necessary for national security or fiscal prudential rules under qualification.[70] The only diverging exception is for requirements by the authorities to antitrust violations, in a time when the EU is accused of investigating several US online services in a manner that liberal US leaders have alleged to be "protectionist".[71]

Ill-defined exceptions in trade agreements

Europe's restrictions on AI (including its privacy rules) are far from the most restrictive regulatory environments in the trading system. The majority of EU countries placing themselves below the average restrictiveness score – while the fast-growing emerging markets tend to score above the EU, including the Asia economies that account for more than half of world's GDP growth,[72] and where the demand for industrial equipment, cars and business services is growing.

But does the EU trade texts actually have any meaningful impact on data flow restrictions around the world. And if not – could the EU agree to a more limited exception without compromising its own legislation?

EU trade texts exempt all 12 countries that impose data localisation against European businesses

Out of the twelve jurisdictions that impose data localisation on EU exporters and investors (figure 5), ten jurisdictions impose them through genuine personal data protection laws. Their restrictions are unconditionally exempt under EU trade texts. Even non-privacy laws that localise data (e.g. the Philippines laws against offshoring, or Nigeria's retail and credit card rules) clearly state privacy as one of the objectives.

In other words, all data localisation restrictions qualify for the exceptions in the EU FTA texts. In all fairness, CPTPP and USMCA provisions categorically exempt any restrictions in the financial sector – e.g. the Philippines, Korea, China and Turkey. Also, the exceptions for national security measures (e.g. for maps and publications in Korea and China) can be argued under any trade agreement, including the WTO.

[68] See EU-Japan EPA., article 8.73

[69] *ibid.*

[70] *ibid.,* article 8.72.2(c)

[71] Ahmed, M., *Obama attacks Europe over technology protectionism*, Financial Times, February 16, 2015

[72] See *inter alia* IMF, Asia's Dynamic Economies continue to lead global growth, 9 May 2017, accessed at: https://www.imf.org/en/News/Articles/2017/05/08/NA050917-Asia-Dynamic-Economies-Continue-to-Lead-Global-Growth; ADB, *Asian Development Outlook 2017*, 2017; World Bank, Global Economic Prospects, 2017

10 out of 12 jurisdictions taking data localisation measures against the EU are doing so using genuine privacy legislation

Figure 5 — Data localisation or storage requirements affecting European exporters

	Country	*Regulatory objective*
Ongoing FTA negotiations with the EU	Indonesia	Privacy regulation (all sectors);[73] ICT regulation covering all online services and public services with mixed objectives.[74]
	Vietnam	Privacy regulation (all sectors);[75] cybersecurity laws with the objective to protect both national security and personal information.[76]
	Malaysia	Privacy regulation (all sectors),[77] but where transfers are permitted under some conditions.
	Philippines	Banking regulation, with the objective of protecting personal information and banking confidentiality.[78]
	India	Privacy regulation (all sectors), but where transfers are permitted under some conditions;[79] regulations on public and government information with "accessibility" objectives.[80]
FTAs in place with the EU (without disciplines on localisation)	Canada	Privacy regulation (on data held by public bodies in some provinces).[81]
	Korea	Privacy regulation, (all sectors)[82] but where transfers are permitted under certain conditions; banking regulation to protect personal information and financial records;[83] national security objectives on online maps.[84]
	Mexico	Privacy regulation (all sectors),[85] but where transfers are permitted under certain conditions.
No ongoing negotiations with the EU	China	Privacy regulations (all sectors) with joint objective to protect cybersecurity;[86] also sectoral laws with the objective to protect privacy on personal information in the financial, health and taxi industries;[87] online publication data with public order objectives;[88] mapping data for both privacy and security objectives.[89]
	Russia	Privacy regulation (all sectors).[90]
	Turkey	Privacy regulation (all sectors),[91] but where transfers are permitted under some conditions; e-payment regulations with mixed objectives.[92]
	Nigeria	ICT regulations with mixed objectives;[93] card payment terminals and ATM systems with mixed objectives.[94]

Sources: See footnotes

[73] Indonesia, *Government Regulation No. 82 regarding the Provision of Electronic System and Transaction,* 2012 (with implementing acts, 2016)

[74] Indonesia, *Electronic Information and Transactions Law* (EIT), 2008

[75] Vietnam, *Decree No. 72/2013/ND- CP,* 15 July 2013

[76] Vietnam, *Law 24 on Cybersecurity,* 12 June 2018

[77] Malaysia, *Personal Data Protection Act of 2010*

[78] Philippines, *Resolution No. 2115 of 2015 - Amendments in the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions on the guidelines on outsourcing,* 2015

[79] India, *Information Technology Rules, (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)*, 2011

[80] India, *Public Records Act*, No 69, 1993

[81] Nova Scotia, Personal Information International Disclosure Protection Act, S.N.S. 2006; British Columbia, Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996; Quebec, Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information,

[82] Korea, Personal Information Protection Act, No. 14839, 2014; *Act on Promotion of Information and Communications Network Utilisation and Information Protection*, No. 14839, 2011

[83] Korea, *Utilisation and Protection of Credit Information Act,* No. 14823; *Electronic Financial Transactions Act*, No. 14828, 2012

[84] Korea, *Act on Land Survey, Waterway Survey and Cadastral Records*, No. 12738, 3 June 2014

[85] Mexico, *Federal Law for the Protection of Personal Data in the Possession of Private Parties*, 2011

[86] China, P.R., *GB/T 35273-2017 Information Technology – Personal Information Security Specification*, 2018; *Cybersecurity Law*, 1 June 2017

[87] China, P.R., *Notice to Urge Banking Financial Institutions to Protect Personal Financial Information*, 2011; *Administrative Measures for Population Health Information (For Trial Implementation),* 2011; *Interim Measures for the Administration of Online Taxi Booking Business Operations and Services*, 2016.

[88] China, P.R., *Administrative Regulations for Online Publishing Services*, 2016

[89] China, P.R., *Map Management Regulations,* 2017;

[90] Russia, *On Making Amendments to Certain Laws of The Russian Federation Regarding Clarification of the Order of Processing of Personal Data in Information and Telecommunication Networks*, Fz-242, 21 July 2014

[91] Turkey, *Law on Protection of Personal Data*, No. 6698, 2016

[92] Turkey, *Payment Services and Electronic Money Institutions Law*, No. 6493, 2015

[93] Nigeria, *Guidelines on Nigerian Content Development in Information and Communications Technology*, 2014

[94] Nigeria, *Guidelines on Point-of-Sale Card Acceptance Services*, 2013

The CPTPP and USMCA agreements could however address other data restrictions, especially for restrictions that offer few or no exceptions – e.g. Russia, China, Nigeria or Indonesia. Several least developing countries are also yet enacted privacy laws and neither fulfil the requirement to adopt a legal framework to protect personal information, nor the more specific requirements on user protection under the USMCA.

But are the wide-reaching EU exceptions necessary to protect its own privacy regime – or could the EU agree to either CPTPP or USMCA?

The EU GDPR fulfils the requirement to maintain a legal framework taking into international guidelines, which is easily fulfilled. In fact, one of the international frameworks referenced by USMCA (2013 OECD Privacy Framework) is even modelled after EU legislation.[95]

Also, EU law builds on a user-centric model that empowers citizens to decide what happens to her data, opposed to a government censor calling the shots. Letting the users themselves determine whether they agree to the risks of processing or transfer is consistent with the CPTPP principles of consumer's free choice,[96] and applies to profiling or automated decisions involving AI.[97]

CPTPP acknowledges that governments may have their own regulatory requirements on the transfer of information yet should *endeavour* to have non-discriminatory regime,[98] while USMCA requires such restrictions to be necessary and proportional to the risks presented.[99]As EU obligations apply to all businesses regardless they are domestic or foreign, these conditions by default non-discriminatory. The consent requirements for international transfers does not distinguish between countries of origin and is available to all businesses,[100] in a manner that is consistent with the "most favoured nation" principle in trade law.[101]

The EU also offers other legal instruments for transfer besides consent, including adequacy decisions that allow transfers to entire jurisdictions.[102] If the EU engaged in "arbitrary or unjustifiable, disguised protectionism",[103] it violates not just CPTPP or USMCA provisions, but also the obligations under its own laws. This does not oblige the EU to grant adequacy. Each jurisdiction offers different levels of privacy protection. The EU merely needs to engage in a dialogue – and it is difficult to envisage a situation where the EU even refuses to explain its laws to a third country.

EU privacy rules would stand up to a legal challenge under any of the current trade agreements.

In sum – the EU privacy regime would stand up to a legal challenge under the most ambitious trade agreements currently available. The EU and other jurisdictions provide the legal certainties necessary to use AI, while its own trade instruments are inadequate to deal with the emerging markets. Also, many of the restrictions are imposed by the major markets. Due to their political systems however, they could never come into question for a two-way adequacy (like what the EU achieved with Japan), making a potent trade instrument the only tool available.

[95] 2013 APEC Privacy Framework, article 70; OECD Privacy Framework, article 17 and 18.
[96] *supra* note .
[97] GDPR, article 22
[98] CPTPP, article 11
[99] USMCA, article 19.8.3
[100] *ibid*., article 46
[101] GATT, article III
[102] GDPR, article 45
[103] CPTPP, article 14.11.3a; USMCA, article 19.11.2a

Conclusion

Although the use of AI is still in its early stages, its deployment depends on a number of sub-systems of regulations like data collection and IPRs. AI is also used for heavily regulated activities, like driving on public roads or financial services. AI needs access to personal and public data to become useful, with properly defined rights and liability within reasonable boundaries.

Trade agreements help to keep this regulatory system competitive and non-discriminatory. Each of the agreements – CPTPP, USMCA and EU Japan EPA – have incrementally brought more clarity. However, each agreement has also brought ever-wider exceptions.

However, AI is not the first overlap between trade and domestic regulations. But fundamental rights are a new issue – and the policymakers in the field are less accustomed to trade commitments and overplaying their risks. After all, the EU has continued its most controversial and allegedly anti-scientific regulations despite being challenged at the WTO.[104]

Trade and privacy are divided by some inherent structural differences: Trade agreements typically empower foreign exporters to safeguard their market access rather than the consumers. Meanwhile, privacy empowers users to enforce their fundamental rights. Interestingly, the CPTPP introduced some new language (albeit non-binding) emphasising the rights of the users to access services of their choice. Philosophically, the CPTPP is more in line with EU privacy laws – which is based on user choice – than Europe's own trade agreements.

If such rules were binding, an individual – not the government or the business – could challenge discriminatory online restrictions imposed on a lawful service in its domestic courts. Similarly, trade agreements could require its signatories to empower the users, i.e. maintain at least explicit user consent as a legal condition for cross-border data flows.

Finally, this report has illustrated what's at stake for an export economy like Europe. In AI, it is not just the size of the home market that matter but also the openness: The Chinese search engine Baidu failed to deliver a viable product on the Japanese market using its Chinese search algorithms, despite the many linguistic commonalities and an unprecedented marketing budget.[105]

China is currently making major efforts to champion AI and big data using public investments, including a US$ 2 billion development in Beijing –[106] but there are no guarantees they will succeed. Similarly, Japan failed to make their protocol for mobile internet (*i-mode)* a global standard by overspecialising on the home market – a mistake the literature calls "Galapagos syndrome" after the island with its own biodiversity that evolved in isolation and cannot survive outside of its habitat.[107]

[104] WTO, European Union—Measures concerning meat and meat products, DS26.

[105] Millward, After 8 years of failing, Baidu shuts Japan search engine, Tech in Asia, April 17, 2015

[106] Reuters, Beijing to build $2 billion AI research park: Xinhua, January 3, 2018, accessed at: https://www.reuters.com/article/us-china-artificial-intelligence/beijing-to-build-2-billion-ai-research-park-xinhua-idUSKBN1ES0B8

[107] Hiroko Tabuchi, Why Japan's Cellphones Haven't Gone Global, New York Times, July 19, 2009, accessed at: https://www.nytimes.com/2009/07/20/technology/20cell.html?em