



THE EU AS A GLOBAL DIGITAL ACTOR

Prof. Elaine Fahey
Institute for the Study of European Law (ISEL)
City Law School, City St. Georges, University of London

Binding regulation of data anathema to Big Tech

and integrated artificial intelligence systems.
(c) Moratorium.--

(1) In general.--Except as provided in paragraph (2), no State or political subdivision thereof may enforce, during the 10-year period beginning on the date of the enactment of this Act, any law or regulation of that State or a political subdivision thereof limiting, restricting, or otherwise regulating artificial intelligence models, artificial intelligence systems, or automated decision systems entered into interstate commerce.

(2) Rule of construction.--Paragraph (1) may not be construed to prohibit the enforcement of--

(A) any law or regulation that--

(i) the primary purpose and effect of which is to--

(I) remove legal impediments to, or facilitate the deployment or operation of, an artificial intelligence model, artificial intelligence system, or automated decision system; or

(II) streamline licensing, permitting, routing, zoning, procurement, or reporting procedures in a manner that facilitates the adoption of artificial intelligence models, artificial intelligence systems, or automated decision systems;

(ii) does not impose any substantive design, performance, data-handling, documentation, civil liability, taxation, fee, or other requirement on artificial intelligence models, artificial intelligence systems, or automated decision systems unless such requirement--

(I) is imposed under Federal law;

or

(II) in the case of a requirement imposed under a generally applicable law, is imposed in the same manner on models and systems, other than artificial intelligence models, artificial intelligence systems, and automated decision systems, that provide comparable functions to artificial intelligence models,

■ H.R.1 - One Big Beautiful Bill Act 119th Congress (2025-2026)

OVERVIEW OF LECTURE

- I. Conceptual issues of digital external relations law**
- II. Recent regional/ bilateral issues**
- III. EU digital trade issues**
- IV. Digital strategic autonomy: protectionism of the internal market**
- V. EU in IO's**

RESEARCH QUESTION

- Critically evaluating the 'constitutional' contours (lower case c' of digital external relations as a concept, field or metaphor
- Increasingly fundamental rights challenges from soft law/ protectionism
- Move focus from effects/ reach/ influence

**Just what is digital law- a proliferating mass of regulatory regimes without appropriate calibration?
(Streinz)**



THE 'CONSTITUTIONAL' CONTOURS OF THE EU DIGITAL AGENDA

- Legal sources
 - EU data policy documents
 - Treaty; Article 16 TFEU; Article 114 TFEU a lot; Article 215 TFEU CFSP
 - Charter
 - Secondary law
 - eg Decision (CFSP) 2019/797 — restrictive measures against cyber-attacks threatening the EU or its MS; Regulation (EU) 2019/796 — restrictive measures against cyber-attacks threatening the EU or its MS
 - A plethora of alphabet law GDPR, DSA, DMA, DA
 - Industrial policy European Chips Act; Cyber Resilience, Act, Cyber Security Act, Cyber Solidarity Act; European Critical Raw Materials Act ; AI Act?
- Declarations
- International agreements
- Eg Data flow and transfer agreements eg TFTP/ PNR

TWIN WEAKNESSES OF EU LAW

INFORMALISATION OF EU EXTERNAL RELATIONS

- eg External migration
 - Collective act of the MS in EU–Turkey statement;
 - MoU -Tunisia;
 - Combination of different instruments -Egypt;
 - Joint declaration -Mauritania.
- Not ‘international agreements’ re Article 218 TFEU

FRAGILITY OF GREAT TRANSITIONS GREEN/ DIGITAL(?)

- **Green Deal**
 - ‘...Internal Market law and its underlying principles are not necessarily sufficiently capable, resilient and future-proof to contribute to the “green transition”’.
 - de Vries, Sybe A. and Neergaard, Ulla, (2025). Recalibration of EU Internal Market Law Paradigms in Light of the EU Green Deal
- **NGEU**
 - ‘NGEU modelmeasured against the yardsticks of democratic governance, financial accountability and efficient allocation of the limited Union resources, the model does not look like a blueprint to emulate.’
 - Päivi Leino-Sandberg Why the NGEU Model is Ill-Suited for Responding to the EU’s Current Geopolitical Challenges (2025)

THE FUTURE OF EU DIGITAL POLICY - COUNCIL CONCLUSIONS (2024)- INTERNATIONAL DIMENSIONS

Development and strengthening of bilateral and regional digital partnerships and digital trade agreements

Multilateral and multistakeholder fora

Promote EU strategic interests; stronger, more strategic, coherent and effective EU policy and action

Intl cooperation

Strengthen the EU's leadership in global digital affairs

Coherent EU Digital Diplomacy

Develop an EU strategy on the multistakeholder governance of the Internet

Increase European leadership in the development of global standards

05 June 2025 Joint Communication on an International Digital Strategy for the EU

1. DIGITAL AS A CORE ELEMENT OF THE EU'S EXTERNAL ACTION

At the current geopolitical juncture, the EU remains a reliable and predictable partner, committed to strengthening its existing relations with allies globally, and forging new mutually beneficial partnerships with those willing to work towards shared objectives. The EU's support to the rules-based global order, aligned with the values of democracy, rule of law and fundamental rights, is steadfast.

The EU's growing network of bilateral and regional partnerships allows the EU to be stronger on the world stage, building coalitions in pursuit of shared objectives in key international fora and organisations. From shaping norms in multilateral fora to deepening bilateral partnerships, the EU aims to make progress on concrete and immediate priorities, protecting and promoting the EU's strategic interests.¹

As emphasised by the Draghi report², the increasing productivity gap between the EU and the United States since the mid-1990s is largely explained by the superior ability of the US to innovate, scale-up globally and succeed in the tech sector. The EU also faces the risk of weaponisation of its technological and economic dependencies and the risk of critical technology leakage. As outlined in the ProtectEU Strategy³, the lines between offline and online



VERY SOFT INTERNATIONAL ECONOMIC LAW ERA

- **Bilateral and soft law:**
 - The transatlantic EU-US Trade & Technology Council (TTC)
 - EU-India TTC
- **Digital Asian Partnerships**
 - TTC as part of a series of soft law digital partnerships including Japan (May 2022), Singapore (February 2023), and South Korea (November 2022)
 - Now DTAs



->Parliamentary exclusion, non-binding standards, outside of Article 218 TFEU, unenforceable ???

DIGITAL EXTERNAL RELATIONS A LIMITED/ UNLIMITED FIELD OF EU LAW COMPETENCES?

SOME KEY ELEMENTS

- **Digital governance incl GDPR**
 - Has external data transfer aspects
 - Heavy dominance of data transfers puts pressure on GDPR law, but not defined there and adequacy a procedure outside of ordinary law-making
- **Cyber**
 - Cybersecurity orienting to internal market law?
 - Cyber Sanctions harden to
 - Cyber in trade agreements ; soft law partnerships
- **AFSJ**
 - PNR agreements under Article 218 TEFEU but is that right?
- **Industrial policy (?)**
 - eg Net zero, Cloud computing



CAPTURING DIGITAL ACTORNESS

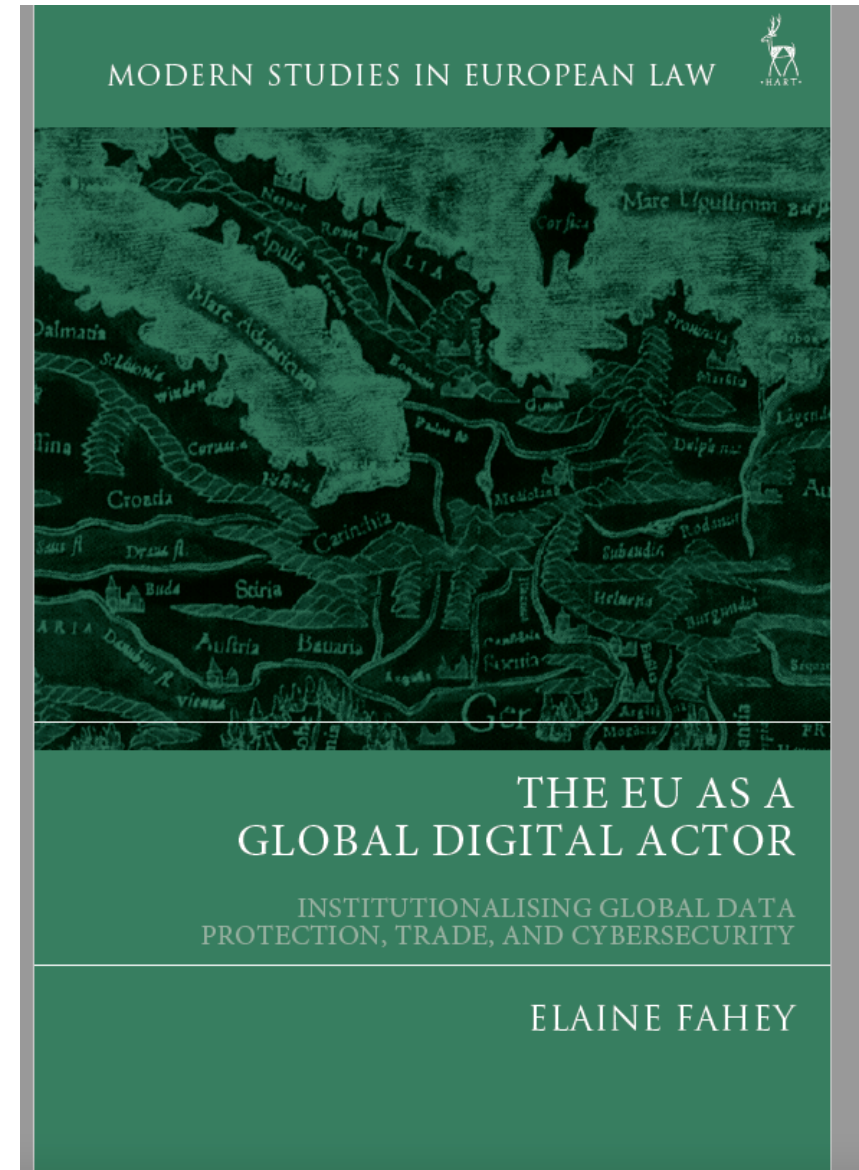
No universal formula for data issues in a trade agreement

->cybersecurity, intellectual property, transparency to frictionless movement of tech workers.

No global privacy or cybersecurity treaty

EU has had 'first-mover' advantage in many domains of data

I argue that more holistic focus is needed upon data- & beyond GDPR
i.e. upon cross-cutting areas of data governance, transfer, digital trade, cyber regulation, law enforcement and the internet of things.





EU INDUSTRIAL POLICY & DIGITAL EXTERNAL RELATIONS: THE EU'S GEOECONOMIC TURN

- ‚BACK WITH A TWIST‘ (MEUNIER, HELDT)- BUT LEGAL IMPLICATIONS?
- European integration started as Industrial Policy - MS led; coal and steel
- 1950s-1970s focused on economic objectives, mostly keeping a technological edge
- 1980s-2010s: industrial policy replaced by competition policy
- 2020s: Industrial emerging with a security twist

COVID-19 and the Ukraine war revealed vulnerabilities in supply chains and energy

Geopolitical shifts and shocks



DIGITAL STRATEGIC AUTONOMY AS A LEGAL CONCEPT, FIELD OR METAPHOR?

- → The digital transformation/ digitalisation has considerably more weakish legal foundations?
 - Overstretching of internal market Article 114 TFEU
 - Complex contours?
 - Sovereignty and (strategic) autonomy and overuse of internal market
Fahey and Poli; Beaucillon and Poli
- Increasingly broad understanding of term sanction (eg Lonardo), maybe same can be said for the *digital* ?

- **3 examples of digital strategic autonomy as de facto de jure external relations**

CYBER: THE SLOW THEN RAPID LEGALISATION OF EU CYBERSECURITY

Rapid legalisation, agenfication, institutionalisation of EU cybersecurity?

- Weaker synergies with trade
- Clumsy mix internal market/ CFSP

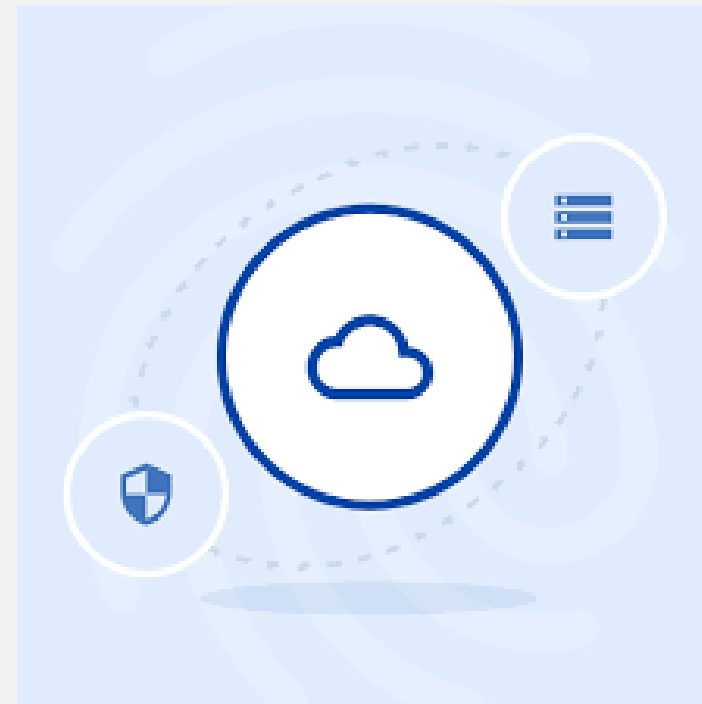


CYBER REGULATION DEVELOPMENTS

- Cybersecurity Act; Cyber Resilience Act; Cyber Solidarity Act; Internet of Things (IoT)
 - EU moves beyond putting obligations for users to require that manufacturers design products that keep data safe
 - e.g. Article 114 TFEU;
 - Commission Delegated Regulation (EU) 2022/30; IoT- Cyber Resilience Act 2022 common cybersecurity standards for products with digital elements
 - US work

CLOUD COMPUTING

- **EU's attempts to regulate cloud computing in Digital Markets Act, the Digital Services Act, Data Act using Article 114 TFEU**
 - EU is relying on its data sovereignty agenda to offset the lack of competitiveness of its cloud ecosystem
 - Vast majority of data produced in the West is stored in US servers (Propp)
- **EU - first jurisdiction that has adopted sector-specific rules for cloud computing**
 - Eg DSA definition of 'online platform' does not fit cloud services.
 - not clear what 'public' means.
 - includes cloud services that do not necessarily qualify as online platforms eg OneDrive



NET-ZERO 'CLEAN TECH' REG

- Framed again as internal market, couched in external relations and protectionism
 - Regulation (EU) 2024/1735 of on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem Based on Article 114 TFEU
 - Seeks to boost EU green-tech manufacturing against rivals from China and US
- NZIA encompasses final products, components, and machinery necessary for manufacturing net-zero technologies
 - homegrown clean tech can cover at least 40% of the bloc's demands by 2030.



COMPATIBILITY WITH OTHER EU LAW

MARKET POWERS?

- EU relies heavily on (hard) internal market powers for all aspects of eg digital strategic autonomy, digital sovereignty measures and even recently defence measures, with external relations elements
 - Article 114 TFEU

**REGIONAL /
BILATERAL**



EU-US TRADE AND TECHNOLOGY COUNCIL OUTCOMES?

- The EU-US Trade and Technology (TTC) has been a key element of transatlantic cooperation in trade and technology in global challenges.
 - opposed to regulatory cooperation - fixated upon global challenges.
 - Critical Minerals Agreement? Mineral Security Partnership?

DETAILED MAPPING EU-US-US AI TAXONOMY

- OECD/ G20 advances considered
- NIST learning from EU AI Board
- Terminology and social science usage

TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management 1 December 2022

1. Background

Tangible global leadership by the United States and the European Union can provide scalable, science-based methods to advance trustworthy approaches to AI that serve all people in responsible, equitable, and beneficial ways. Effective risk management and assessment can help earn and increase trust in the development, deployment, and use of AI systems. Recognizing the power of AI to address the world's challenges, we also acknowledge AI systems entail risk. By minimizing the negative impacts of AI systems on individuals, culture, the economy, societies, and the planet, we can maximize the positive impacts and benefits of AI systems that support the shared values underpinning like-minded democracies. Towards that goal, the U.S.-EU Joint Statement of the Trade and Technology Council (May 2022) expressed an intention to develop a joint roadmap ("Joint Roadmap") on evaluation and measurement tools for trustworthy AI and risk management.

This Joint Roadmap aims to guide the development of tools, methodologies, and approaches to AI risk management and trustworthy AI by the EU and the United States and to advance our shared interest in supporting international standardization efforts and promoting trustworthy AI on the basis of a shared dedication to democratic values and human rights. The roadmap takes practical steps to advance trustworthy AI and uphold our shared commitment to the Organisation for Economic Co-operation and Development (OECD) Recommendation on AI.

2. Risk-based approaches: Bringing EU and U.S. approaches closer

The United States and EU acknowledge that a risk-based approach and a focus on trustworthy AI systems can provide people with confidence in AI-based solutions, while inspiring enterprises to develop trustworthy AI technologies. This approach supports common values, protects the rights and dignity of people, sustains the planet, and encourages market innovation. Both parties are pursuing risk-based approaches that operationalize these values.

Both sides apply risk-based approaches that consider the combination of societal and technical factors (socio-technical perspective) to advance trustworthy AI. EU examples are represented in the proposed EU AI Act and the work of the High-Level Expert Group (HLEG) on AI. United States examples can be seen in the National Institute of Standards and Technology (NIST) draft AI Risk Management Framework as well as the White House Office of Science and Technology Policy

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK 2022

- A new two-tier redress system to investigate & resolve complaints of Europeans on access of data by U.S. Intelligence authorities, incl Data Protection Review Court
- Removal of Democratic members Privacy and Civil Liberties Oversight Board (PCLOB)
- *Latombe v. Commission* General Court Case T-553/23
- Adequacy decision



The European Commission and the United States reached an agreement in principle for a **Trans-Atlantic Data Privacy Framework**.

Key principles

- ◆ Based on the new framework, **data will be able to flow freely and safely** between the EU and participating U.S. companies
- ◆ A new set of rules and **binding safeguards to limit access to data** by U.S. intelligence authorities to what is **necessary and proportionate** to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- ◆ **A new two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a **Data Protection Review Court**
- ◆ **Strong obligations for companies** processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- ◆ **Specific monitoring and review mechanisms**



Benefits of the deal

- ◆ Adequate protection of Europeans' data transferred to the US, addressing the ruling of the European Court of Justice (*Schrems II*)
- ◆ Safe and secure data flows
- ◆ Durable and reliable legal basis
- ◆ Competitive digital economy and economic cooperation
- ◆ Continued data flows worth over 6000 billion USD annually



EU-INDIA TTC

- India –EU held first Trade and Technology Council (TTC) meeting on 16 May 2023
 - “tackle challenges at the nexus of trade, trusted technology, and security”
 - strengthen India-EU strategic partnership
- August 2023, India enacted the much-awaited Digital Personal Data Protection Act, 2023 (the DPDP Act)
 - India capture of DMA equivalent
 - India was high localisation data user/actor-? GDPR esque



EU AT THE WTO, COE, UN IN DIGITAL MATTERS

A decorative graphic consisting of several thick, concentric black arcs that curve from the bottom right towards the center of the image. The background is a solid purple color.



WTO, EU AND DIGITAL TRADE AGREEMENTS

- **No settled definition of ‘digital trade’ or ‘electronic commerce’**
- Out of 465 agreements signed between 2000 and 2024, 231 have provisions on e-commerce/digital trade and 135 contain dedicated e-commerce/digital trade chapters (**Burri et al 2025**)
- **Archaic understanding goods v. services & digital trade at WTO, predate digitization**
- Currently, 91 WTO Members are participating in the eJSI negotiations with the goal of concluding an agreement on digital trade
- EU....

BURRI 2025

- New generation of Digital Economy Agreements (DEAs)- increasing number of issues covered incl sensitive area
 - what their real impact is
 - whether reduce / exacerbate regulatory fragmentation
 - differing stances towards the regulation of the data-driven economy, eg US, the EU and China, difficulties to align views



LATEST NOTABLE EU TRADE NEGOTIATIONS AND THEIR DIGITAL LINKS

- **EU-India**

- 2022, EU relaunched negotiations with India for FTA
 - Investment Protection Agreement and an Agreement on Geographical Indications (GIs).
- 2024- EU-India Commission alleged India's WTO inconsistent tariffs on ICT goods
- EU Enforcement Regulation to enforce India's compliance 2023 EU India new Trade and Technology Council (TTC)

- **Philippines**

- 18 March 2024 EU and the Philippines negotiations for FTA
- Global Gateway

- **South Korea**

- 2025 EU - Korea Digital Trade Agreement (DTA)

- **Singapore**

- 2025 EU-Singapore Digital Trade Agreement (DTA)

EU HORIZONTAL STRATEGY ON DATA FLOWS (2018)

Horizontal provisions for cross-border data flows and for personal data protection *(in EU trade and investment agreements)*

Article A

Cross-border data flows

1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:

- (i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;
- (ii) requiring the localisation of data in the Party's territory for storage or processing;
- (iii) prohibiting storage or processing in the territory of the other Party;
- (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.

2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.

1

Article B

Protection of personal data and privacy

Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.

Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.

For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person.

For greater certainty, the Investment Court System does not apply to the provisions in Articles A and B.

Article X

Cooperation on regulatory issues with regard to digital trade¹

1. *The parties shall maintain a dialogue on regulatory issues raised by digital trade, which shall inter alia address the following issues:*
 - *the recognition and facilitation of interoperable cross-border electronic trust and authentication services;*
 - *the treatment of direct marketing communications;*
 - *the protection of consumers in the ambit of electronic commerce; and*
 - *any other issue relevant for the development of digital trade.*
2. *Such cooperation shall focus on exchange of information on the Parties' respective legislation on these issues as well as on the implementation of such legislation.*
3. For greater certainty, this provision shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data.

- Horizontal exception on protection data
- Unties EU data protection from EU external policy
- Australia, Chile, Indonesia, Mexico, New Zealand, Tunisia
- Replacement EU-Japan EPA clause

DIGITAL TRADE AGREEMENT (DTA) WITH SINGAPORE (MAY 2025)

- BUILDING on their deep and longstanding partnership, based on the common principles and values reflected in the Partnership and Cooperation Agreement between the European Union and its Member States, of the one part, and the Republic of Singapore, of the other part, done at Brussels, on 19 October 2018 (hereinafter referred to as the "Partnership and Cooperation Agreement"), by giving effect to its provisions on trade;
 - DESIRING to deepen the free trade area established by the Free Trade Agreement between the European Union and the Republic of Singapore¹, done at Brussels, on 19 October 2018 (hereinafter referred to as the "Free Trade Agreement");
 - RECOGNISING the EU–Singapore Digital Partnership (hereinafter referred to as the "Digital Partnership"), signed on 1 February 2023, as an initiative to promote cooperation between the Union and Singapore, in a variety of areas of the digital economy and to create opportunities for joint initiatives and efforts in new and emerging areas of the digital economy
-
- DTA - self-standing agreement –separate to the EU-Singapore Free Trade Agreement and the EU-Singapore Investment Protection Agreement
-
- ‘The objective ...is to facilitate digital trade in goods and services between the Parties in accordance with the provisions of this Agreement.’

NGOS ON ERA OF DTAs & EU LAW

ETUC

- TAs should not negatively impact the ability of the EU to enforce its own digital laws, and for member states to go beyond minimum EU standards.
- ...Data flows and protection: the EU has model clauses on data flows. However, in DTAs, the EU sometimes adapts to the partner's needs unduly...

EDRI

- 'EU is signing digital trade deals that could undermine fundamental rights and block oversight of software systems shaping our lives.'
- **What does 'digital trade' really mean?**
- ...rules are negotiated in opaque processes without meaningful civil society engagement
- The EU is now signing stand-alone Digital Trade Agreements (DTAs) for the first time, starting with Singapore and South Korea. These agreements pick up and expand on a problematic trend: already in previous free trade agreements, digital chapters – dealing with issues like data flows and software governance – had started to appear, raising concerns about regulatory autonomy and rights protection. ...

Free Trade Agreements with comprehensive digital trade chapters concluded with UK, New Zealand, Chile & ongoing with India, Indonesia, Thailand, Philippines and Malaysia

its principles.

ARTICLE 12.5

Protection of personal data and privacy

1. Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to enhancing consumer confidence and trust in digital trade.
2. Each Party may adopt or maintain measures it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this Agreement shall affect the protection of personal data and privacy afforded by the Parties' respective measures.

WORLD'S FIRST MULTILATERAL AI TREATY

COUNCIL OF EUROPE: AI CONVENTION V. EU AI ACT

- Commission signed the Council of Europe Framework Convention on Artificial Intelligence (AI) on behalf of the EU after FRA work for 18 months
- AI Framework Convention protects all existing International and European Human Rights
 - Art. 5 safeguard the “integrity, independence and effectiveness of democratic institutions and processes”,
 - AI Framework Convention excludes national security and defence from scope.
 - Applies to public authorities or private entities acting on their behalf



EU AI Act 2024 v. COE?

- EU AI Act 2024 narrower, follows product safety legislation
 - **AI Act** (EU Regulation 2024/1689 on AI) does not deal with contractual or extra-contractual liability issues.
 - Extra-contractual liability for AI recently introduced with **EU new Directive for manufacturer's liability for defected products** (EU Directive 2024/2853)
- AI Act 2024 stepped model with different obligations based on risk categories defined by the Act
- gap

- The external reach and effects of the EU's AI Act
- Risk-based approach AI Act v. human rights-based approach of the Treaty
- AIA creates novel data governance obligations *not* grounded in data protection concerns

UN: The Global Digital Compact (GDC)

- Increasingly non-binding UN Global compacts on key global challenges eg migration, refugees, digital
 - Negotiated by 193 Member States and informed by global consultations,
 - first comprehensive framework for global digital governance.
 - objectives, principles, commitments and actions to develop an open, free and secure digital future for all.
- **‘EU will remain actively involved in the GDC implementation work to defend its achievements, while ensuring non-duplication of efforts and maximizing synergies with the existing global digital architecture, including the Internet Governance framework’.**



EU LAW V. UN GLOBAL DIGITAL COMPACT

- Voluntary non-binding international initiative
- Considerably lower data protection standards
- Divergence between EU ambitions and global regulatory practices?



CONCLUSIONS

- Constitutional matrix of digital external relations law ever expanding
 - Increasingly international organisation initiatives at WTO, CoE and UN level demonstrate downwards pressures upon standards and values
 - The constitutional challenge of the digitisation shift where more subjects/ objects to regulate beyond users
 - Hard law/ soft law conundrum of EU digital law
 - Industrial policy protection vis DSA a help/ hindrance?
 - Fragmentation, competition, downwards IO experiments?

