ETUC Position on EU Digital Trade Agreements with 3rd countries

Adopted at the Executive Committee meeting of 10-11 December 2024

According to the European Commission, digital trade covers trade in goods and services enabled by the internet and other information and communication technologies. This includes goods or services ordered online that are later delivered at home or through the internet such as apps on smartphones and computers; use of technologies such as those used for tracking in real time; transfer of data across borders (e.g. data stored in the cloud when working online).

The EU is the world's largest exporter of services, half of which are digital services. Thus the EU a major responsibility for the sustainable development and safeguarding public interests of this sector. To this end, the EU has been negotiating stand-alone Digital Trade Agreements (DTAs), especially where existing trade agreements with partner countries do not include digital trade chapters. With DTAs, the EU does not only seek to open up markets and improve access to e-commerce, but claims also to secure EU consumer protection, protecting consumers' data and privacy – which the Commission maintains to be non-negotiable, but the European Data Protection Supervisor has expressed concerns that in practice this is not the case and said protections are sometimes traded away.

In summer 2024, EU and Singapore concluded a DTA, complementing the existing EU-Singapore FTA. With this additional deal the EU aspires to set a global standard for digital trade rules and cross-border data flows. The agreement could be presented to the European Parliament for ratification as early as January 2025. The EU is also negotiating similar agreements with South Korea, the Philippines and Thailand.

This position sets out the ETUC guiding principles this and future DTAs will be measured against to represent a gold standard. Some of these principles, where appropriate, would also extend to e-commerce negotiations under the WTO framework. This position complements existing resolutions on trade and other relevant policy areas.

Right to regulate and economic policy space: DTAs must preserve and not undermine the policy space to adopt regulatory and other measures, including through social dialogue and collective bargaining, to address new challenges in the digital economy, including the protection of public health data, the public control and resilience of digital infrastructure, regional value creation, AI and anchoring the 'human in control' principle. DTAs 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.

Workers' rights: DTAs should not prevent enforcement of workers' rights or indeed the improvement of working conditions. To this end, DTAs should not prohibit obligations for companies to have legal and/or physical presence in the territory of the parties to the agreement.

European Trade Union Confederation | Esther Lynch, General Secretary |
Bld du Jardin Botanique 20 - 1000 Brussels | +32 (0)475 601 501 | etuc@etuc.org | www.etuc.org

DTAs should not prevent workers from claiming a right to the data and the economic value they produce: trade rules should not cement companies' exclusive ownership of the data collected. Workers' participation to data governance should also be guaranteed. Moreover, digital corporations that abuse workers' rights should not be rewarded with trade liberalisation and greater market access rights via DTAs.

Data flows and protection: the EU has model clauses on data flows. However, in DTAs, the EU sometimes adapts to the partner's needs: this can result in dilution of protection of workers' rights including data privacy, increases legal uncertainty as well as exposure to trade dispute over digital rights. This must be prevented: the EU should limit itself to granting data adequacy decisions as these are unilateral measures that can be withdrawn anytime. DTAs should not undermine the European Data Protection Supervisor and national authorities. Trade agreements should not set the rules for cross-border data flow without guarantees that EU GDPR would always take precedence over the terms of trade. Public interests and data protection must always take precedence over offensive commercial interests.

Access to source code must not be prohibited for public authorities, which may need said access for specific legal cases, such as intellectual property disputes, or for more general reasons, like ensuring economic stability or investigating potential biases and fraudulent practices. Regulatory bodies' ability to ensure that companies comply with legal requirements could be diminished with a blanket ban on access to source code. Also, free access to the source code must be ensured before the implementation of AI systems in the workplace. Blocking access to source code, if enshrined in DTAs, would undermine the transparency and checks and balances needed to prevent the misuse of algorithmic management.

Tax on big tech: no clauses in DTAs should prevent directly or indirectly parties to the agreement from taxing the profit of big tech. One thing is to ban customs duties on electronic transmissions like email exchanges, another is to prevent a state from introducing digital services tax or increasing the existing level of corporation tax. Bans on data localisation also hinder authorities' ability to assess corporate profit, for instance by preventing requirements to store accounting data locally, and risk undermining the EU public Country-by-Country Reporting Directive.

Public services and digitalisation: DTAs should not lead to privatisation of public services, including through creeping private-public partnerships. Also, there are risks of undermining public values and national security in some cases; of increasing dependence from certain dominant providers in others; of impeding oversight of algorithmic decision-making to determine access to benefits and other public services; of 'paying twice' for what is our own data as citizens and patients. Similarly, DTAs should not entrench the use of national security or public order to water down or prevent further regulation and public scrutiny (as it happened for the Council of Europe framework convention on AI). ETUC believes that public services and infrastructures must be carved out from trade and investment negotiations – this applies also to DTAs, and at the very least data collected through public service provision should remain in public ownership.