# EU DIGITAL TRADE RULES: UNDERMINING ATTEMPTS TO REIN IN BIG TECH

By Deborah James

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

This report was commissioned by The Left in the European Parliament

March 2023

The author would like to thank Bram Vranken, Cecilia Olivet, Cedric Leterme, Christina Colclough, Georgios Altintzis, Jane Kelsey, Kristina Irion, Léa Auffret, Maryant Fernandez, Parminder Jeet Singh, Penny Clarke, Rashmi Banga, Roland Kulke, Sanya Reid Smith, Theo Morrissey, Nicolas Strauch and others for their thoughtful analysis, comments, and revisions. All errors and omissions remain the responsibility of the author.

GUE/NGL
THE LEFT
IN THE EUROPEAN PARLIAMENT

B-1047 Brussels, Belgium
+32 (0)2 283 23 01
left-communications@europarl.europa.eu
www.left.eu

# PREFACE

Teachers, doctors, politicians and journalists have recently found a common source of concern: ChatGPT. They all discovered the potential negative - and still by far unknown - impact of the fast developing artificial intelligence (AI) technology. Teachers are worried that students can use AI to produce essays undetectable for plagiarism which could seriously hamper their analytical development. Doctors are anxious about patients following a diagnosis provided through AI without it being confirmed by any medical specialist. Politicians fear that ChatGPT will challenge the real substance of honest democratic discussions and interfere with their dialogues with citizens, including in decision-making. Journalists are concerned that AI-produced articles are presented as journalism - without any checks for accuracy or for sources, leading to a potential surge in fake news.

Everyone is pointing at the same pitfalls. On the one hand, AI trains itself by drawing enormous amount of data from the internet but it cannot distinguish between what is fact and what is fake. On the other hand, there is an inherent racial, gender and class bias in existing data on the internet, so the AI system is prone to replicate the bias it draws on, deepening existing inequalities.

AI is spreading like wildfire. While recognising its benefits is easier, **the potential harms of AI applications are not yet fully known**, nor are enough safeguards in place to deal with them. At the moment, Big Tech companies are way ahead of laws and regulation, and are operating in one of the most unregulated sectors of the global economy. **Governments have started identifying possible risks emerging form this lack of regulation and are developing solutions**. The EU, for example, is advancing legislation such as Digital Services Act, the Digital Markets Act, the Data Act, the Data Governance Act and the Artificial Intelligence Act, which aim to rein in the power of US and Chinese companies dominating the sector.

Nonetheless, **Big Tech companies are set in preventing governments' regulatory efforts to continue to accumulate data. One of the most powerful tools available to them are international trade agreements.** Clauses dictating free flow of data, bans on data localisation and non-disclosure of algorithms hand over to multinational companies a complete monopoly over data, while stripping governments and other actors in society from any potential oversight over algorithms and data use.

**It seems inconsistent that, on the one hand, the EU introduces legislation to regulate the global digital economy and Big Tech companies; while on the other, it is promoting trade deals which will inevitably strengthen Big Tech's influence against government regulation.**

This inconsistency has led to some calls within academia to develop an international governance regime for the digital economy[1]. This could entail the establishment of a core club of nations championing new digital trade agreements to advance a trusted digital environment, setting standards and rules. This regime could also develop basic criteria based on commonly agreed values - in a democratic sense of giving everybody the chance and the right to take part in the development of digital economies and their impacts on daily life.

There is a growing recognition that digital technologies are transforming the global trading system and will scramble the borders dividing sectors in both our macro-and micro-economies, shattering the division between traditional and new industries. In this context, the market alone will not resolve the emerging disputes and confrontations. Governance to of the digital economies will be - and already is - needed.

1 Peter F. Cowhey and Jonathon D. Aronson, "Digital DNA: disruption and the challenges for global governance", Oxford University Press, New York, 2017.

Shoshana Zuboff argued that the digitalized society is defined by the institutionalisation of a "pathological" division of knowledge. Big Tech corporations from the US and China get to access and process more information, feeding into their decisions over individuals - and consequently - societies.

It is necessary to re-think how rules and governance structures are shaped, jumpstarting a global process that can take into account the needs and rights of peoples in the global South and ensuring their participation in setting new standards.

There is very little assessment of the interrelation between the new proposed EU's digital economy legislation and how it relates to the current EU's digital trade policy. In light of this, The Left group in the European Parliament commissioned this report to explore this nexus as well as to map the possible effects of the EU's digital trade agreements for European society.

Even though the preliminary findings are worrying, I hope they will lead to a productive participation in the collective task of re-shaping the digital era's trade rules and governance structures. The findings of this study seem to suggest a lack of policy coherence, indicating that the EU could be undoing with one hand what it is doing with the other.

We invite fellow Parliamentarians, the European Commission, national regulators, watchdogs, academics, trade unions and civil society organisations to read this report, hoping that it will contribute to new standards and regulations benefitting society at large.

Helmut Scholz

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

This report shows how Big Tech corporations are working to constrain the ability of European Union (EU) democratic bodies to regulate their activities in the public interest through "trade" agreements, which are binding and permanent.

Digitalization is the defining economic transformation of our time. The benefits to society are well-known, but the harms caused from the expansion of Big Tech are still being understood. The EU has started to recognise the urgent need rein in some of Big Tech's most pernicious practices. The Digital Services Act (DSA), the Digital Markets Act (DMA), along with the Data Act, the Data Governance Act (DGA) and the Artificial Intelligence Act (AI Act) are first steps towards ensuring that the digital sector of the economy operates under the same framework of fair play and the public interest as the rest of the economy.

The same EU that is advancing new laws governing the digital economy is simultaneously promoting a digital trade policy that contradicts, and would severely constrain, current and future public interest policymaking in the EU and beyond.

Through a number of bilateral and regional trade agreements, Big Tech is seeking to maintain a policy environment which favours private control of technological resources and practices, and data, for supernormal profit. Control over data – and in particular, the ability to transfer data across borders – and keeping their algorithms or source codes secret are the top goals of Big Tech in any "digital trade" agreement.

The EU has finalized trade agreements with a dedicated digital trade chapter with Canada, Singapore, Vietnam, Japan, the UK, Mexico, Chile, Mercosur, and New Zealand. And it is currently negotiating digital trade chapters with Indonesia, Australia, India, the region of Eastern and Southern Africa (ESA), and plurilaterally in the WTO.

This research analyses the most dangerous clauses included in the EU digital trade agenda ("free" flow of data, bans on data localisation and non-disclosure of source code). It identifies **10 REASONS WHY IT WILL BE HARMFUL FOR EUROPEAN SOCIETY, EUROPE'S GREEN AGENDA AND DEMOCRACY AT LARGE:**

## 1. THE EU'S ABILITY TO TAX THE MOST PROFITABLE CORPORATIONS IN THE HISTORY OF THE WORLD WOULD BE CONSTRAINED BY THE DIGITAL TRADE RULES

Digital firms have seen their profits soar during the last few years as a result of a sharp increase in cross-border digital activities. Yet the taxes they pay remain extremely low, including in Europe. A company like Uber, for instance, can easily shift "highest value creation" from the country of its operation to a tax haven like Ireland from where the backend software and analytics are shown to be provided. The European Commission already in 2018 proposed to improve unfair taxation for the digital economy. And, in 2021, the EU joined the global tax agreement reached at the OECD. Yet, EU's efforts to tax Big Tech could be contradicted by its own digital trade policies.

Nearly all EU trade agreements with digital provisions include a ban on customs duties on electronic transmissions (ETs). This means that while importers of products such as cars, watches, and agricultural goods are subject to duties, or trade taxes, if the same good is electronic – as in the case of books, movies, or music – states are prohibited from imposing taxes. A key argument used by defenders of this ban is that it benefits EU digital export small and medium-sized enterprises (SMEs). But large U.S.-based corporations, including Apple (music), Netflix (movies), and Amazon (books) benefit from the moratorium far more than any SMEs in the EU.

And it is not just direct taxes that Big Tech seeks to prevent through trade agreements. A provision banning governments from being able to require a copy of data to be held locally makes it more difficult for governments to assess corporate profit taxes. Tax havens are increasingly used by Big Tech as "data havens" to prevent government access to data that could have tax implications otherwise.

## 2. QUALITY, ACCESSIBLE PUBLIC SERVICES WOULD BE UNDERMINED BY BIG TECH'S CONTROL OVER DIGITALIZATION OF SERVICES

Maintaining a strong public services sector in Europe will require strengthening algorithmic accountability and up-skilling digital knowledge among public workers. It will also require the use of large data sets by the public sector to improve education, health, transportation, water and electricity distribution, and other public services. Digitalization of public services often involves public-private partnerships with Big Tech corporations. If the data collection of the public service, or the provision of the service itself, is privatized, then so is the data. In order to obtain the data to improve public services, public services should maintain the right to access and control the data produced through any partnerships with private companies. Under the proposed EU digital trade rules barring states from requiring the localisation of data in the Party's territory for storage or processing, the required disclosure from companies could be challenged under trade agreements.

## 3. EU CITIZENS' DATA PRIVACY RIGHTS AND CONSUMER PROTECTIONS COULD BE UNDERMINED BY THE DIGITAL TRADE RULES

The landmark legislation of the GDPR published in 2016 set the global standard for the fundamental rights of data privacy and data protection. Recent trade agreements, like the ones with the UK and New Zealand, include a clause that aims to safeguard the protection of personal data and privacy. However, there are serious doubts that the "safeguards" included will indeed protect personal privacy. Subsequent to the publication of the EU-United Kingdom Trade and Cooperation Agreement (EU-UK TCA), the European Data Protection Supervisor (EDPS) stated that "[...] the TCA creates legal uncertainty about the EU's position on the protection of personal data in the context of trade agreements and risks creating friction with the EU data protection legal framework".

## 4. THE EFFORTS OF EUROPEANS TO ENSURE THE RIGHTS OF LOCAL MINORITIES AGAINST DISCRIMINATION WOULD BE UNDERMINED BY THE DIGITAL TRADE RULES

There is a growing body of evidence that AI can exacerbate discrimination and cause harm, either through faulty algorithms which "learn" patterns based on past inequities, or by exacerbating inequalities found in data sets used for training. In 2019, the EC published a White Paper on Artificial Intelligence which recognised that the increasing use of algorithms in Europe poses specific risks in terms of fundamental rights and in particular in terms of equality and non-discrimination. Further, recent studies have shown that source codes and algorithms which are inter-connected and learn from themselves (machine-learning) can lead to many undesired outcomes which include discrimination based on income, color and gender.

But digital trade proposals proscribe states from requiring source code disclosure. They do contain exceptions to allow disclosure of source codes and algorithms to requesting judicial or regulatory authorities for investigations, and the EU-New Zealand FTA uniquely expands this to include discrimination and bias. But the Conference of the Federal and State Ministers for Equality of Germany "pointed out that, due to the complexity of the matter, it seemed unrealistic that those affected would be able to detect and pursue algorithmic discrimination." Furthermore, transparency remedies must also be available for affected parties, researchers, critical engineers, advocates, trade union stewards, and the general public – not just for governments. If algorithmic systems might violate fundamental and human rights to be free of discrimination, AI systems should have to be proven not to do so in advance of their deployment – not after harms are suffered.

## 5. THE EU'S GREEN DEAL AGENDA, ESSENTIAL TO ENSURING FUTURE SUSTAINABILITY, WOULD BE HAMPERED UNDER THE DIGITAL TRADE RULES

The EU Green Deal promotes new technological innovation to resolve the world's climate crisis. But for the entire world to make the necessary transitions, transfers of climate-reducing technology innovations to ensure their global use will be required. Bans on source code disclosure, and other forms of technology transfer, will render the achievement of the Paris Agreement impossible for many countries.

Countries also need tax revenue (for example, from taxing Big Tech) in order to fund their transition. Big Tech's proposals to limit the ability of states to tax their activities will reduce those needed investments. The hyper-concentrated and data hungry digital economy promoted by Big Tech and the proposed digital trade rules is also radically at odds with the fight against global warming. The digital economy uses 10% of the world's electricity and generates nearly 4% of global CO2 emissions, almost twice as much as the civil aviation sector. Sustainable digitalization cannot co-exist with huge digital monopolies pushing for ever more collection, storing and processing of data on a global scale.

## 6. THE EU'S DIGITAL TRADE AGENDA WOULD CONSTRAIN POLICYMAKERS' AND REGULATORS' ABILITY TO REIN IN BIG TECH'S MARKET DOMINANCE AND ENSURE A LEVEL PLAYING FIELD

European regulators and legislators have become well aware of the negative impacts of Big Tech's monopoly practices and powers. Europe has engaged in the most extensive enforcement actions to reduce Big Tech's market dominance to set a level playing field to ensure fair competition, especially for SMEs. But certain provisions in digital trade agreements, in particular the Understanding on Computer and Related Services (UCRS), bans on source code disclosure requirements, interoperability provisions, and bans on local presence requirements, could undermine these efforts.

The UCRS would guarantee digital infrastructure firms have virtually unrestricted access into countries and rights to operate there with very limited regulation. Countries that agree to the EU's UCRS agree to include market access commitments for "computer systems, programming including source codes and algorithms, maintaining computer systems and software, and processing and storage of data." But it would also include those services yet to be invented. They could not limit the size or scope of a foreign company's operations. Applying open-ended disciplines which restrict competition policy remedies to all digital services would benefit the monopolistic practices of Big Tech.

Anti-competitive practices using algorithms are ubiquitous in the online retail sector, where companies like Amazon ensure that their search algorithms privilege their own products or services above those of others. The exceptions included in digital trade rules will not be enough to curb those practices. Those rules still require a suspicion, as they relate to specific cases, and cannot require disclosure as a general rule– individuals must know that they are being harmed and have a suspicion that it is because of the algorithm and convince the regulatory agency.

## 7. SMALL BUSINESSES IN THE EU WOULD BE HIGHLY DISADVANTAGED UNDER THE EU'S DIGITAL TRADE RULES

In 2021, 99.8 percent of all enterprises in the EU-27 non-financial business sector (NFBS) were SMEs. They employed 83 million people. The vast majority of EU-based SMEs that sell online use Big Tech online platforms to reach consumers. SMEs are dependent on platforms' algorithms in terms of how their products are ranked in search results or are otherwise advertised. Businesses using Big Tech platforms do not have access to the data on their own customers and resulting from their activity on the gatekeeper's platform, making it impossible for them to compete in a fair market – while the Big Tech platform can use such data for its own business purposes. Digital trade provisions that bar states from being able to require algorithmic transparency or that copies of data be stored locally constrain remedies for these problems.

Furthermore, European proposals in trade agreements propose to fully liberalize the market access for computer and related services so digital infrastructure firms have virtually unrestricted access into countries and rights to operate with very limited regulation. While some may see an opportunity to gain access to foreign markets for European firms, the first mover and scale advantages of U.S.-based Big Tech means they would likely consolidate their dominance rather than SMEs. In that context, it is difficult to see any scope for protecting or supporting European SMEs.

## 8. THE EU'S DIGITAL INDUSTRIALIZATION AGENDA WOULD BE HAMPERED IF BIG TECH WERE ABLE TO UPLOAD THEIR INTERESTS INTO DIGITAL TRADE AGREEMENTS

Europe's digital industrialisation strategy relies on improving access to data, developing technology and infrastructure, and appropriate regulation. However, the digital trade strategy clashes with Europe's aims. A great amount of data that is generated in Europe is held by foreign-based companies. European drivers and riders produce data for Uber, European consumers make purchasing choices on Amazon, which the U.S.-based corporations then use for their own business strategies. Digital rules would prevent governments from requiring companies to share this data or requiring data to be held locally. As a result, Europe's ability to access the large troves of data required to scale digital industrialization will be compromised.

The creation of digital infrastructures, in particular data centres used for cloud computing, is key for Europe's digital industrialization strategy. Currently, U.S.-based companies now control nearly 72 percent of the European cloud storage market. France and Germany have promoted local data centre infrastructure, and the EU proposed the creation of a European cloud, Gaia-X. But the EU's digital trade rules against data localization proscribe states from being able to require the use of computing facilities or network elements in the Party's territory for storage or processing. If the EU could not ensure that EU-based data infrastructure is utilized, then cloud carriers such as Amazon, Google, and Microsoft will pursue their data storage and processing needs in cheaper data havens, not in Europe.

## 9. THE DIGITAL RULES WOULD REDUCE THE ABILITY OF EUROPEAN AGENCIES TO ENSURE FINANCIAL STABILITY, DIGITAL INTEROPERABILITY, AND CYBERSECURITY SUCH AS REGARDING THE "INTERNET OF THINGS"

Preserving policy space for regulation is crucial to ensuring widespread benefits from digitalization and guaranteeing European fundamental rights in the digital sphere. The digital trade rules are broad and all-encompassing. Public interest regulation would be subject to challenges with only the narrow window of limited exceptions. Future-proofing the ability to regulate according to evolving political and economic landscapes is crucial.

For example, digital trade rules could affect financial regulation and cybersecurity. Decisions in the financial sector are increasingly determined by algorithms which must be subject to regulatory oversight and public scrutiny. Decisions such as who will get a loan for a house or who will be awarded insurance based on credit risks, are increasingly made by data and algorithms. Also, the growing automation of stock markets operations pose enormous risks in terms of financial stability. Despite exceptions for prudential measures, trade provisions bar governments from requiring disclosure of source code in order to ascertain the security of the financial sector and would preclude the regulatory oversight necessary to guarantee financial security.

The Internet of things (IoT) market for digitally connected devices is an emerging concern for cybersecurity specialists. European governments are increasing cybersecurity legislation on IoT devices in order to protect sensitive consumer (including financial) data and safety. Cybersecurity regulation will require standards such as two factor authentication (TFA), and the disclosure of source code to evaluate high-risk algorithms and cybersecurity measures. But the provisions of digital trade rules promoted by the EU would bar states from being able to require necessary disclosure of source code. The exceptions – including in the most recent EU-NZ FTA – still far short of the enormity of the urgent need for more public oversight.

## 10. THE POWER IMBALANCE BETWEEN BIG TECH AND WORKERS WOULD BE TILTED EVEN FURTHER AGAINST WORKING PEOPLE, IF BIG TECH GETS ITS WAY IN REWRITING THE RULES THAT GOVERN DIGITALIZATION

Digital trade proposals in trade agreements represent an effort by Big Tech to further consolidate that upward distribution of income from labour to capital. In discussions on the future of work, the emphasis on job retraining and skill-based technological growth can be useful but should not be a distraction. The most important aspect in shaping who will benefit from expanded technological use will be the policy environment in which that technology is utilized. If workers are not guaranteed their fundamental rights, freedom, and autonomy in digitalised workplaces, and if workers do not have a governance stake in the data produced by workers, and instead this data is allowed to be "owned" by the collecting corporation, it will permanently skew the balance of power in further favour of corporations. Whether workers should have economic rights to the data they help produce is a subject being debated. Locking data related commitments under trade agreement will make any such thing impossible, likely leading to a permanent suppression of labour's collective bargaining power in a digital age.

Big Tech applies extensive political pressure in Europe, and it appears that their lobby activities have resulted in a deregulatory trade agenda that primarily benefits Silicon Valley.

The thinking that more digital trade means that there must be rules governing this trade is misplaced. Trade agreements inherently limit states' rights to regulate economic behaviour. Yet, governments should have the space to advance regulations to ensure human and fundamental rights in the digital economy; promote the use of data and digitalization for the public good; and promote digital industrialization. The EU must ensure that its trade agreements do not constrain its ability to implement stronger regulation of Big Tech to protect workers, consumers, SMEs, minorities, sustainability, and fundamental rights in the digital sphere.

# 1.

# INTRODUCTION: THE EU'S DIGITAL TRADE AGENDA: WHY DOES IT MATTER?

Digitalization is the defining economic transformation of our time. The benefits to society from increased digital efficiency and access are well-known. But the harms caused to society from the expansion of Big Tech's decision-making over our lives as workers, consumers, small businesses, and citizens, as well as our democracies as a whole, are no longer being ignored.

That's why legislators and regulators in the EU have begun a long process of developing appropriate public interest oversight over the actions of Big Tech behemoths and the digital economy more generally.

While the improvement in technology is welcome, the policy environment within which the technologies are utilized defines who will gain, and who may suffer in the long run. This policy environment is the choice of lawmakers and regulators, rather than being an unseen force under which the winners and losers are inevitable.

Heretofore, policy makers have allowed technology companies to accelerate the incursion of technology into our lives without a priori regulation. While Big Tech are now the largest and most powerful corporations in the history of the world, they are also the least-regulated of any sector.

Big Tech companies have long argued that regulation would stifle innovation. But the reality is that today, the largest and most powerful technology corporations act not as innovators but as monopolists, seeking to prevent competition and dominate markets. They accomplish this through a business model that depends on mass surveillance of users, by monopolizing data and data processing as well as digital infrastructures, and through the control of the use of technology through their proprietary algorithms.

In particular, they have sought to commodify and control the production, harvesting, and use of data for private profit, rather than to allow the public the opportunity to use digitalization and data for the common social, environmental, and economic good, and by evading the application of human and fundamental rights and public interest regulation in the technological sphere.

Lawmakers, law enforcement, the media, trade unions, digital rights advocates, and society at large have engaged in robust debate about some of the negative impacts of Big Tech corporations on society. The EU in particular has recognized these harms and started to advance new laws designed to rein in some of Big Tech's most pernicious practices. The Digital Services Act (DSA), the Digital Markets Act (DMA), along with the Data Act (DA), the Data Governance Act (DGA) and the Artificial Intelligence Act (AI Act) are first steps towards ensuring that the digital sector of the economy operates under the same framework of fair play and the public interest as the rest of the economy.

Big Tech corporations have not taken this burgeoning interest in regulation lying down. They have engaged in massive efforts to limit the scope and coverage of the new laws, in the EU and around the world.

While their lobbying efforts are well-known, what is less well-known is that they are also engaged in a parallel effort to constrain lawmakers' freedom and obligations to regulate them in the public interest, now and forever, through influencing governments to create binding international "trade" agreements in their interests.

Corporations use international "trade" agreements to achieve their agendas because they are the policymaking process most beholden to the business sector and the least open to other public interest stakeholders (such as labour unions, privacy advocates, anti-discrimination groups, and others.)

They are legally binding, which recommendations from the Organization for Economic Cooperation and Development (OECD) or statements by the G20 are not. Big Tech also prefers using trade agreements to set disciplines on national legislation because although countries can change governments, it is nearly impossible to change trade agreements as they are inter-governmentally negotiated permanent treaties. While "trade" agreements used to focus on tariffs, today the vast majority of the provisions give rights to trade, which are exercised by trading firms, and restrict the ability of states to regulate those firms in the specified areas.

Specifically, Big Tech has successfully convinced the European Commission to take on its long-term business agenda as the EU agenda on digital trade. Many of the provisions in this agenda affect domestic policymaking on myriad issues beyond "trade", as will be shown below.

However, this agenda is little debated or understood by lawmakers, the media, or the public in general. Nevertheless, this agenda serves as the blueprint for the EU's efforts to secure "digital trade" agreements with target countries in bilateral agreements, as well as globally in the World Trade Organization (WTO).

This "trade" agenda is in direct contradiction to the current efforts of European leaders and lawmakers to uphold human and fundamental rights in the digital sphere; to reduce harms caused by Big Tech; and to ensure that technology benefits society overall. Given the requirement that EU external policy remain in line with its principles, documents, and existing law, there is a pressing need to fundamentally re-think the EU's approach to digital trade agreements.

Over the last five years, development advocates and academics have identified untold anti-development impacts of the provisions in these proposed agreements.[2] A main focus is the provisions that allow corporations to transfer data across borders while at the same time prohibiting states from being able to require the use of local data servers, or copies of the data to be held locally. Critics have argued that these provisions would prevent the ability of developing countries to use data produced by workers, consumers, businesses, and citizens in their own countries for their own development and would thus forestall digital industrialization in developing countries.[3] They have argued that the provisions would instead fundamentally benefit Big Tech corporations based mainly in the U.S. They would thus harm working people and SMEs, as well as disempowering legislators and regulators, in developing countries.[4]

Development advocates and UN agencies have also shown that provisions like banning governments from being able to require the disclosure of source code will benefit knowledge accumulation in developed countries at the expense of technological advancement in the developing world.[5] Concerns have also been raised regarding problems with source code secrecy resulting in the abrogation of democracy, such as with regards to bad actors' ability to exploit Facebook's algorithms to unduly influence outcomes in many elections.[6]

What is less recognised is that many of these same "trade" provisions would actually have immense negative impacts on workers, consumers, businesses, citizens, and governments within Europe.

**This preliminary study thus aims to shed light on the EU's digital trade agenda and its potential impacts on European society, particularly in view of the recent regulatory directions of the suite of new laws governing the digital economy.**

2 Rashmi Banga, 'Joint Statement Initiative on E-Commerce (JSI): Economic and Fiscal Implications for the South,' *UNCTAD* Research Paper No. 58 (February 2021), https://www.twn.my/announcement/UNCTAD%20Re%20Paper%2058_022021.pdf. See also UNCTAD DITC and DTL, 'What is at Stake for Developing Countries in Trade Negotiations on E-commerce?: The Case of the Joint Statement Initiative,' UNCTAD (2021), https://unctad.org/webflyer/what-stake-developing-countries-trade-negotiations-e-commerce; and Jane Kelsey, 'How a TPP-style E-commerce outcome in the WTO would endanger the development dimension of the GATS acquis (and Potentially the WTO)', Journal of International Economic Law 21, no. 2 (June 2018): 273-295, https://doi.org/10.1093/jiel/jgy024.

3 Renata Ávila Pinto, 'Digital Sovereignty or Digital Colonialism? New Tensions of Privacy, Security and National Policies,' *Sur International Journal on Human Rights 15*, no. 27 (July 2018): 15-27, https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-renata-avila-pinto.pdf.

4 Rashmi Banga and Richard Kozul-Wright, 'South-South Digital Cooperation for Industrialization: A Regional Integration Agenda,' *UNCTAD* (April 2018), https://unctad.org/system/files/official-document/gdsecidc2018d1_en.pdf

5 Sanya Reid Smith, 'Some Preliminary Implications of WTO Source Code Proposal,' *Third World Network* WTO MC11 Briefing Paper (December 2017), https://www.twn.my/MC11/briefings/BP4.pdf; and Banga, 'JSI on E-Commerce,' UNCTAD (2021).

6 Craig Silverman, Ryan Mac, and Pranav Dixit, "I Have Blood on My Hands': A Whistleblower Says Facebook Ignored Global Political Manipulation,' *BuzzFeed News* (September 2020), https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo.

# 2.

# THE EU'S DIGITAL TRADE AGREEMENTS

The U.S. hired a top Big Tech lobbyist to create its digital trade policy. It subsequently introduced the first digital trade proposals in the WTO in 2016, which greatly mirrored corporate wish lists. The EU followed suit. The EU and the U.S. were unsuccessful in their bid to convince WTO members generally to launch new negotiations on digital trade at the Buenos Aires Ministerial in December 2017 but later announced their intention to do so anyway.[7]

In March 2019, fewer than half of the WTO membership launched "plurilateral" negotiations on digital trade amongst themselves.[8] The EU is an active participant and has tabled several proposals.[9] Negotiations have continued on a regular basis, in tight coordination with business lobbies. In contravention of WTO practice, negotiating texts are held in secret, but draft texts were leaked.[10] Negotiations are accelerating towards the next WTO Ministerial Conference, to be held in February 2024.[11]

The EU has advanced its digital trade policy in parallel[12] through a number of bilateral and regional agreements and negotiations.[13]

The EU has finalized trade agreements with a dedicated digital trade chapter with Canada, Singapore, Vietnam, Japan, the UK, Mexico, Chile, Mercosur, and New Zealand. Out of these, only the first five are in force so far.

Researchers have noted that EU digital trade provisions have expanded over time.[14] Initially, the digital agenda mainly consisted of a moratorium on customs duties on electronic transmissions. However, from 2016 onwards, they incorporated more and more regulatory issues including provisions on cross border data transfers and source code,[15] which is a key part of algorithmic systems.[16]

The EU is currently negotiating trade agreements with a dedicated digital trade chapter bilaterally with Indonesia, Australia, India, the region of Eastern and Southern Africa (ESA), and plurilaterally in the WTO.[17]

In addition, the EU will soon launch negotiations for digital partnership agreements with Singapore and South Korea.[18] In October 2022, it started negotiating an update of the digital trade chapter with Japan to include cross border data transfer provisions, an issue that was left out of the treaty signed in 2018.[19]

7 Kelsey, 'How a TPP-Style E-commerce Outcome in WTO…,' Journal of IntlEcon Law (2018).
8 This undertaking rests on a shaky legal basis given the multilateral nature of the WTO. See Jane Kelsey, 'The Illegitimacy of Joint Statement Initiatives and Their Systemic Implications for the WTO,' *Journal of International Economic Law 25*, no. 1 (March 2022): 2–24, https://doi.org/10.1093/jiel/jqac004.
9 See the EU's proposal in the JSI on e-commerce. EU delegation, 'Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce (Document # 19-2880),' WTO INF/ECOM/22 (April 2019), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=253794,253801,253802,253751,253696,253697,253698,253699,253560,252791&CurrentCatalogueIdIndex=6&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.
10 'WTO Electronic Commerce Negotiations: Updated Consolidated Negotiating Text – September 2021,' WTO INF/ECON/62/Rev.2 (September 2021), https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text_september_2021.pdf.
11 World Trade Organization, 'E-commerce talks resume following summer break, Mauritius joins the initiative,' *WTO* press release, (September 2022), https://www.wto.org/english/news_e/news22_e/ecom_16sep22_e.htm
12 European Commission Directorate-General for Trade, 'Communication: Trade Policy Review - An Open, Sustainable and Assertive Trade Policy,' European Commission COM/2021/66 final (February 2021), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:66:FIN. Also see European Commission, 'Shaping Europe's digital future,' EU flyer (February 2020): section 3, https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278; and see European Commission, 'Communication: 2030 Digital Compass: the European way for the Digital Decade,' European Commission COM/2021/118 final (March 2021), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.
13 Sofia Scasserra and Carolina Martínez Elebi, 'Digital Colonialism: Analysis of Europe's trade agenda,' *TransNational Institute* (October 2021), https://www.tni.org/files/publication-downloads/digital-colonialism-report-tni_en.pdf.
14 Michele Fink, 'Legal analysis of international trade law and digital trade,' European Parliament briefing PE 603.517 requested by the INTA Committee (November 2020), https://op.europa.eu/en/publication-detail/-/publication/18173e33-2954-11eb-9d7e-01aa75ed71a1/language-en/format-PDF/source-172804686.
15 Pierre Sauvé and Marta Soprana, 'Chapter 11 The Evolution of the EU Digital Trade Policy,' in *Law and Practice of the Common Commercial Policy*. The first 10 years after the Treaty of Lisbon (Leiden: Brill | Nijhoff, December 2020): 290, https://doi.org/10.1163/9789004393417_013; Scasserra and Elebi, 'Digital Colonialism: Europe's trade agenda,' TransNational Institute (2021).
16 Dorobantu et al. writes: "Source code refers to the lines of code written by programmers to instruct a machine to perform a given task. Source code is usually written in a text file, it is readable by humans, and it uses a programming language," and that, "Pieces of code that contain a series of steps that need to be followed in order to solve a computational problem are often called algorithms." Cosmina Dorobantu, Florian Ostmann, and Christina Hitrova, 'Source code disclosure: A primer for trade negotiators', in *Addressing Impediments to Digital Trade* (London: CEPR Press, April 2021): 105-140, https://ssrn.com/abstract=3877039.
17 European Commission, 'Overview of FTA and other Trade Negotiations,' commission draft version 1.15 (January 2023), https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/a7aab8e0-085d-4e36-826f-cbe8e913cf13/details; European Commission, 'Overview of Economic Partnership Agreements,' commission draft version 1.9 (January 2023), https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/10ca1b54-d672-430b-aed4-8b25b4b9c2ee/details.
18 European Commission, 'Overview of FTA and other Trade Negotiations' (January 2023).
19 European Commission Directorate-General for Trade, 'EU and Japan start negotiations to include rules on cross-border data flows in their Economic Partnership Agreement,' European Commission Trade News (October 2022), https://policy.trade.ec.europa.eu/news/eu-and-japan-start-negotiations-include-rules-cross-border-data-flows-their-economic-partnership-2022-10-07_en.

# 3.

# THE MOST DANGEROUS EU DIGITAL TRADE RULES: DATA FLOWS, DATA LOCALISATION AND NON-DISCLOSURE OF SOURCE CODE

Early digital trade agreements focused on what are essentially taxes on trade: barring states from being able to impose customs duties on electronic transmissions. There is no agreement in the WTO on what constitutes an electronic transmission,[20] but a 2016 WTO Note listed digitized films, music, printed matter, computer software and video games.[21] Others have tried to expand this to digital services.[22]

But the EU's newer agreements go far beyond traditional trade issues. The new agenda focuses on the desire of Big Tech corporations to monopolize data and control its use. Control over data – and in particular, the ability to transfer data across borders – and keeping their algorithms or source codes secret are the top goals of Big Tech in any "digital trade" agreement.

The use of artificial intelligence (AI) has increased exponentially in recent years. AI involves using large data sets to train computers to make decisions. Computers make the decisions based on the data provided to them, based on instructions from the algorithms based on source code. Larger sets of data increase the ability of companies to train computers to use the algorithmic systems for far more accurate outcomes. Thus, the corporation that will dominate an industry in the future is the one which will have the greatest access to and capacity to manage enormous aggregations of data combined with proprietary algorithms that produce the most profit.

The global AI market was valued at 35 billion euros in 2020. This figure was expected to increase to 45.5 billion euros in 2021 and reach a staggering 349 billion euros by 2028, growing at a compound annual growth rate of 33.6 percent.[23] More than 58,000 AI-related patents were registered in the U.S. between November 2016 and 2021, making it the global leader in AI.[24] Corporations are thus focused on harvesting, collecting, storing, and processing massive troves of data from their own subsidiaries as well as purchasing data from other sources.

The newer generation of "trade" agreements includes these top provisions from the corporate lobby wish lists:

- constraining states from restricting corporations' ability to transfer data across borders;
- prohibiting the ability of states to require that foreign firms process data and/or store it locally; and

20 Indonesia secured a definition at MC11 that does not include content. Developing countries have challenged the scope of electronic transmissions in the WTO because of its potentially devastating impact on their revenue if it applies to digitalized content. But FTAs gloss over that problem and make it permanent, such as in Art X.6 in the EU-New Zealand FTA.

21 WTO General Council, 'Fiscal implications of the customs moratorium on electronic transmissions: the case of digitisable goods (Doc # 16-6961),' WTO JOB/GC/114 (December 2016). For a fuller discussion of the issue, see the previously cited Banga, 'JSI on E-Commerce,' UNCTAD (2021).

22 See Hosuk Lee-Makiyama and Badri Narayanan Gopalakrishnan, 'The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions,' *European Centre for International Political Economy* Policy Brief no. 3 (August 2019), https://ecipe.org/publications/moratorium/.

23 Figures from Global Newswire, 'Artificial Intelligence (AI) Market to Hit USD 360.36 Billion by 2028; Surging Innovation in Artificial Internet of Things (AIoT) to Augment Growth: Fortune Business Insights™,' Fortune Business Insights (September 2021), https://www.globenewswire.com/news-release/2021/09/16/2298078/0/en/Artificial-Intelligence-AI-Market-to-Hit-USD-360-36-Billion-by-2028-Surging-Innovation-in-Artificial-Internet-of-Things-AIoT-to-Augment-Growth-Fortune-Business-Insights.html; currencies converted 14 November 2022 using https://www.bloomberg.com/quote/USDEUR:CUR.

24 Naomi Davies, 'Index shows US is winning the AI race – but for how long?,' Investment Monitor (November 2021), https://www.investmentmonitor.ai/ai/ai-index-us-china-artificial-intelligence.

- prohibiting states from requiring that companies disclose source code, which is a core part of algorithmic systems.[25]

## CROSS BORDER DATA TRANSFERS

Big Tech often uses the euphemism of "free flow of data" (FFOD) to refer to its cross-border data transfer objectives. But it is clear that the intention is not to flow "freely". Big Tech's intention is for private corporations to appropriate and control all forms of data – no matter who produced it, who processed it, in what state it originated, or how the public might benefit from it – for purely private interest. Article 1 of the horizontal text agreed within the EU for use in digital trade agreements, in its first article on data flows, states that: "[t]he Parties are committed to ensuring cross-border data flow to facilitate trade in the digital economy."[26]

Big Tech corporations are now four of the five largest corporations in the world, by market capitalization.[27] Apple, Microsoft, Alphabet (Google), and Amazon are so highly valued by investors because of the data they hold, and its potential for revenue, among other reasons. The Economist famously concluded in 2017 that data is the world's most valuable resource.[28] Accordingly, in November 2022, Apple had a market capitalization value of 2 trillion euros. Germany (4 trillion euros), France (2.8 trillion euros) and Italy (2 trillion euros)[29] are the only three countries in the EU with GDP in 2021 higher than Apple's market capitalization. Apple's market capitalization is thus higher than the annual output of 24 EU countries.

Since the passage of the landmark General Data Protection Regulation (GDPR),[30] the EU has concretized the primacy of privacy and data protection as essential elements in the EU's digital trade policy.[31] Privacy experts have lamented the inadequate enforcement of the GDPR and continuously call for its strengthening. Nevertheless, it marks a turning point in corporations' unrestricted ability to move data across borders.

The implications of allowing corporations to move data across borders without restrictions go far beyond personal privacy. Over the last 40 or so years, the use of digital technologies has expanded dramatically. While productivity growth in developed economies has been slower in recent decades than in the post-war period, digital technology likely has been an important contribution to the growth that there has been. However, capital owners, rather than people who work, have captured increasing amounts of the income from the expansion in the last four decades.[32]

This is a major source of inequality within societies today. For the EU, the top 10 percent of households received nearly six times the income received by the lowest 50 percent in 2021 – this is after taxes and transfers which make the income distribution less regressive. This is up from 1990, when the top 10 percent received five times the income of the bottom half.[33] Wealth inequality has also increased – the wealthiest decile owned 62 times the net assets of the bottom 50 percent in 1995, rising to 86 times in 2021.[34]

If it is a goal to reverse, or at least halt, this trend, and instead to ensure that workers share in the productivity gains from digitalization, then it will be necessary to ensure that the control of one of the most valuable economic resources in human history is not hijacked by capital – but shared generally among people who work, residents, citizens, and society as a whole.

25 For corporate wish lists, see as example the 'Recommended Priorities for the WTO E-Commerce Discussions July 16, 2018,' signed on by Australian Information Industry Association, DIGITALEUROPE, Information Technology Association of Canada, Information Technology Industry Council, Internet Association, Japan Electronics and Information Technology Industries Association, and National Foreign Trade Council (NFTC). Accessible here: Information Technology Industry Council, 'Business and Tech Groups Release Priorities for WTO E-Commerce Meetings,' ITI press release (July 2018), https://www.itic.org/news-events/news-releases/business-and-tech-groups-release-priorities-for-wto-e-commerce-meetings.

26 Taken from the EU horizontal proposal for 'Provisions on cross-border data flows and protection of personal data and privacy,' EU proposal (July 2018), http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf; also seen in the 'Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part,' abbreviated as EU-UK TCA (April 2021): Title III, Article 201, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.149.01.0010.01.ENG&toc=OJ%3AL%3A2021%3A149%3ATOC.

27 Matthew Johnston, 'Biggest Companies in the World by Market Cap,' Investopedia (September 2022), https://www.investopedia.com/biggest-companies-in-the-world-by-market-cap-5212784.

28 'The world's most valuable resource is no longer oil, but data,' *The Economist* (May 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Others might contest this, arguing for example that water or air is a more valuable resource to humanity.

29 Data source from World Bank, 'World Development Indicators,' WB database, https://databank.worldbank.org/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=; currencies converted on 14 November 2022 using https://www.bloomberg.com/quote/USDEUR:CUR.

30 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) [2016] OJ L119/1 (hereafter 'GDPR').

31 Title III, Article 201 in EU-UK TCA.

32 This can be seen in the declining labour share of income in many economies over the period. A study by OECD researchers found that the labour share fell by an average of 2.5 percentage points across the OECD 1995 to 2014, with two thirds of the examined countries experiencing declines. Cyrille Schwellnus, Andreas Kappeler, and Pierre-Alain Pionnier, 'Decoupling of wages from productivity: Macro-level facts,' OECD Economics Department Working Papers No. 1373 (January 2017), https://www.oecd-ilibrary.org/content/paper/d4764493-en.

33 Weighted by national population; "rdiinc_992_j" and "npopul_999_i" for 27 EU countries (Austria, Belgium, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden) on data from: World Inequality Database (accessed November 11, 2022), https://wid.world/data.

34 "rhweal_992_j_QY" from World Inequality Database (accessed November 11, 2022).

Given the economic value of data, is essential to debate and regulate not just about privacy but about the *economic governance of data*. Should the data produced by residents of a jurisdiction be available for use to promote digital industrialization, jobs, and SMEs locally? Or should it only be controlled by Big Tech? Individuals enjoy human and fundamental rights to privacy and data protection; but the International Covenant on Economic, Social and Cultural Rights (ICESCR) also gives people a collective right to control and use their resources.[35]

Data flows are very different from goods and services flows in international trade. The UN Conference on Trade and Development (UNCTAD)'s 2021 Digital Economy Report[36] has rightly argued that given the multidimensional nature of data, a large proportion of data is not associated with any trade, which makes regulating data via trade agreements problematic. Data flows also require a different treatment from the flow of goods and services as data cannot be traded like goods and services. For example, users may be able to use a foreign online service for free (such as search engines, social media, etc.), but during this process, data generated by and about them can be extracted, processed and monetized.

As data flows include non-tradeable issues like personal protection and privacy and human rights, addressing them in the trade regime would be limiting. Trade negotiations do not involve multi-stakeholders which are especially needed for common understanding on non-trade issues. Further, trade negotiations are more relevant when it comes to reciprocal treatments concerning issues such as tariffs and quotas, etc. But including non-trade issues like privacy and human rights especially in the context of digital technologies like facial recognition and racial discrimination can make trade negotiations more challenging with high probability of them collapsing.

Apart from the above reasons for excluding data flows from trade negotiations, on more practical grounds, data flows differ in nature from international trade flows in many ways. Governance and negotiations in international trade relies heavily on statistics on the type of trade flows, values and location of country of origin and destination on traded goods and services. Such an approach for data flows is extremely challenging if not impossible as there are no official statistics to track data flows or quantify them at the country level.

There are no easy solutions to the conundrum of who should own and control data. The discussions and debates over the current legislative projects in the EU make that crystal clear.[37] What is also clear is that it is unacceptable for Big Tech to claim the de facto ownership of the most valuable resource in history, for itself, without democratic debate or agreement.

## BANS ON DATA LOCALISATION

In addition to being able to move data to whatever jurisdiction suits their private profit motives and preferred regulatory regimes, Big Tech also seeks to ban governments from being able to require even a copy of the data to be held locally. Following the article on cross-border data flows above, the subsequent provision in the horizontal text reads,

"To that end, cross-border data flows shall not be restricted between the Parties by:

a) 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 the Party;

b) *requiring the localisation of data in the Party's territory for storage or processing;*

c) prohibiting storage or processing in the territory of the other Party;

d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory."[38] (Italics added. This same text appears in Article 201 of the EU-United Kingdom Trade and Cooperation Agreement (EU-UK TCA) and the Article X.4 of the EU-New Zealand Free Trade Agreement (EU-NZ FTA)[39].)

35 For example, under the Nagoya Protocol of the Convention on Biological Diversity, developing countries have claimed rights to sharing benefits from data arising from gene sequencing of their flora and fauna.

36 UNCTAD, 'Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow,' United Nations (September 2021), https://unctad.org/system/files/official-document/der2021_en.pdf.

37 Joan Lopez Solano et al, 'Governing data and artificial intelligence for all: Models for sustainable and just data governance,' European Parliament PE 729.533 study (July 2022), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf.

38 Title III, Article 201 in EU-UK TCA.

39 'Free Trade Agreement between the European Union and New Zealand,' abbreviated EU-New Zealand FTA (June 2022). Article X.4 text accessible here: 'Consolidated text of all chapters, including the Preamble,' (June 2022): 168, https://circabc.europa.eu/rest/download/1a0e0689-f705-47f3-88e1-09103b88b58d.

These anti-data-localisation provisions strike at the heart of communities' potential to use data for the public good. In addition to an individual exercising their rights over data they produce, there are reasons why the public has a stake in ensuring availability of collective data for public goods such as ending pandemics or mitigating climate change; why a local community or government (such as a traffic jurisdiction) might want to claim rights to data (such as that of private ridesharing apps) to improve traffic infrastructure; or why communities such as workers might have claims to data such as regarding their own labour, issues elaborated further below.[40]

Data centres are the factories of the digital economy and governments should have the right to promote digital factories within their national boundaries through data localisation policies. The trade rules barring data localisation are leading to a "race to the bottom" as countries are struggling to attract investment into their national boundaries by providing subsidies and incentives in favour of the Big Tech firms. UNCTAD has provided a list of industrial subsidies and incentives provided by U.S. states to attract investments in data centres.[41] These include sales tax exemptions, tax breaks, property tax exemptions, grants and concessional loans, etc.

Throughout these discussions, it is thus important to acknowledge the social, cultural, and other values of data. UNCTAD has recently acknowledged that data is not just an economic resource, but has holistic cultural and social aspects, and thus should not be governed solely by an economic institution,[42] such as the WTO or other trade agreements.

Further, the ICESCR requires the protection of other fundamental rights, such as freedom from discrimination. There is a "right to regulate" provision, for example in the EU-NZ FTA (fnArt X.2), that "affirms" a range of "legitimate public policy objectives" including social services, climate change, and cultural diversity. This provision is declaratory which means that it can only be effectuated through the general exceptions.[43] The EU's approach essentially relies on the inadequate general exceptions to protect those rights.[44] Only the protection of personal data has its dedicated counter-balancing provision which is based on a comprise for horizontal provisions for cross-border data flows and for personal data protection in EU trade and investment agreements reached in 2018.[45]

Corporations should not be able to do an end-run around democratic processes, at a time when citizens, workers, regulators, and legislators are engaging in debates about the value of data and the first wave of necessary regulation on this sector, particularly if the firms' aim is to forestall the ability of governments to ensure broader access to data and its benefits for all.

## NON-DISCLOSURE OF SOURCE CODES

Likewise, there is increasing recognition about the growing use and power of algorithmic decision-making. The current business model of surveillance advertising, dominated increasingly by digital surveillance ads, in which Facebook and Google "get more clicks" (and thus derive greater revenue) from inflammatory and inaccurate information[46] rather than reliable, documented facts and reasonable debate, is unsustainable.[47]

But algorithmic systems, including the human-readable source code, are increasingly determining key aspects of our work lives, our social lives, our financial lives, and our political lives. They are used to make decisions about who gets hired, who gets a loan, at what prices we are offered goods, what electoral ads we see. Invasive surveillance of workers with wearables and office spyware are becoming commonplace. These systems often exacerbate racial, gender, and labour discrimination and can further marginalize the already marginalized.[48] The AI Incidents Database by the Partnership on AI reveals

40 See Parminder Jeet Singh and Anita Gurumurthy, 'Economic Governance of Data: Balancing individualist-property approaches with a community rights framework,' *IT for Change* draft for discussion at Quarterly Roundtable of Data Governance Network (January 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3873141.
41 Banga, 'JSI on E-Commerce,' UNCTAD (2021).
42 UNCTAD, 'Digital Economy Report 2021,' United Nations (2021).
43 According to professor emeritus of law Jane Kelsey, the right to regulate provision has interpretive weight when it comes to matters where governments would rely on an argument about a right to regulate. The R2R wording would have some direct interpretive relevance in the approach taken, for example, in the CPTPP where the data rules have an exception inbuilt for legitimate public policy objectives (but still subject to least restrictive and chapeau tests). In the EU-New Zealand FTA there is no such provision, just a cross-reference to the general exception and the "public policy objectives therein" – which are limited, as set out in Art X.1 of the Exceptions chapter. Note that the general exception is distinct from the much stronger language on personal data and privacy in X.5.
44 Daniel Rangel, 'WTO General Exceptions: Trade Law's Faulty Ivory Tower,' *Public Citizen* (February 2022), https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.
45 Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade', *International Data Privacy Law* 10, no. 3 (August 2020): 201–222, https://doi.org/10.1093/idpl/ipaa003.
46 Yael Eisenstat, 'I Worked on Political Ads at Facebook. They Profit By Manipulating Us,' Washington Post (November 2019), https://www.washingtonpost.com/outlook/2019/11/04/i-worked-political-ads-facebook-they-profit-by-manipulating-us/.
47 Matt Stoller, 'Ad Tech and the News: Background on the Rise of Surveillance Advertising and Its Effects on Journalism,' *Center for Journalism & Liberty* (September 2020), https://static1.squarespace.com/static/5efcb64b1cf16e4c487b2f61/t/5f75107ef21702786068d8a3/1601507762535/adtech-cjl-sept2020.pdf.
48 See Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishers, 2016); and Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press: 2018).

nearly four hundred incidents of harm realized by deployment of algorithmic systems globally, with Facebook, Tesla, Google, Amazon, YouTube and TikTok as the worst repeat offenders.[49] Algorithmic systems that impact society must be subject to public oversight.[50]

Algorithmic systems can be evaluated with either "white box" – including access to the source code – or "black box" testing, which involves various techniques not dependent on analysing the source code of the algorithms.[51] For "black box" testing it is necessary to obtain access to data ingested or produced by algorithmic systems which in turn requires software interfaces for auditing which are expressed in source code. Moreover, scholarly investigations have found that there are many complex situations in which it is either more accurate or more efficient to use testing involving analysing not just the output of the machine's learning but the source code itself.[52] In order to address such situations, it will be necessary to pass legislation requiring ex ante and ex post access to algorithms expressed in source code as a precondition to assess whether algorithmic systems meet regulatory and judicial needs, with regards to competition law, equality law, data protection, financial safety, consumer protections, and other issues; for public procurement purposes (including due diligence, for example for software used in critical national infrastructure such as elections; for transparency and accountability, or other strategic considerations); or to promote innovation and economic development.[53]

Yet the digital trade chapter of the EU-NZ FTA, which contains similar language to many EU deals,[54] states that: "A Party shall not require the transfer of, or access to, the source code of software owned by a natural or juridical person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory."[55] While this clause comes with a number of custom-made exceptions for regulatory and judicial enforcement and even conformity assessments, the legislation which authorizes access to source code for these objectives is not exempted from this rule.

Proponents argue that these source code protections are important to protect against forced technology transfer (usually referencing China). But this is not considered an issue in most of the states that are parties to digital trade agreements.

In the EU-UK TCA there are exceptions for competition remedies, and in Article 207 for "a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online."[56] Earlier agreements had even fewer exceptions for source code disclosure, indicating that perhaps regulators realized that trade officials were circumscribing necessary policy space to address increased decision-making by algorithmic systems.[57] These exceptions have been expanded in the EU-NZ FTA, such as to include non-discrimination and the prevention of bias. However, exceptions for many other social ills that are often a result of algorithmic bias, such as false information, emotional manipulation, and others raised by consumer advocacy organizations,[58] do not appear in the text.

Civil society expert organizations have argued that the included exceptions are inadequate to ensure that algorithms and digital technology comply with EU law. To facilitate true public interest oversight, experts argue that EU trade deals should not foreclose policy space for public scrutiny of algorithms for civil society[59] as well as academics, media, critical engineers[60] and trade unions.[61]

49 Accessible at 'AI Incident Database,' *Responsible AI Collaborative* (accessed January 13, 2022), https://incidentdatabase.ai/entities.
50 Frederick Mostert and Alex Urbelis, 'Social media platforms must abandon algorithmic secrecy', *Financial Times* (June 2021), https://www.ft.com/content/39d69f80-5266-4e22-965f-efbc19d2e776.
51 Kristina Irion, 'AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?,' *German Federation of Consumer Protection Organizations* (vzbv) commissioned study (January 2021), https://doi.org/10.2139/ssrn.3786567.
52 Ibid; also Dorobantu et al, 'Source code disclosure,' in Addressing Impediments (2021). See too: Magdalena Słok-Wódkowska and Joanna Mazur, 'Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code,' *Journal of International Economic Law* 25, no. 1 (March 2022): 91–109, https://doi.org/10.1093/jiel/jgac005.
53 Dorobantu et al, 'Source code disclosure,' in Addressing Impediments (2021).
54 Scasserra and Elebi, 'Digital Colonialism,' TransNational Institute (2021).
55 Chapter XX Digital Trade of the "EU-New Zealand FTA, accessible at https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/0fa614a2-7365-4f91-9bd0-88822fc9a16e/details.
56 Title III, Chapter 3, Article 207: Source Code, in EU-UK TCA.
57 Kristina Irion, 'Algorithms Off-limits? If digital trade law restricts access to source code of software then accountability will suffer,' ACM 2022 Conference on Fairness, Accountability, and Transparency (June 2022): 1561-1570, https://doi.org/10.1145/3531146.3533212.
58 Maryant Fernandez and Sebastien Pant, 'Why it's time to ban surveillance ads,' *BEUC (European Consumer Organisation)* blog (November 2021), https://www.beuc.eu/blog/why-its-time-to-ban-surveillance-ads/.
59 BEUC, "EU-New Zealand Trade Agreement: BEUC reaction to the concluded agreement," *BEUC* position paper (August 2022), https://www.beuc.eu/position-papers/eu-new-zealand-trade-agreement-beuc-reaction.
60 Irion, 'Algorithms Off-limits?,' ACM (2022).
61 Christina Colclough, 'Union Brief: G7 Digital Policy Priorities 2022,' *Why Not Lab* (2022), https://www.thewhynotlab.com/post/reminding-the-g7-workers-rights-are-human-rights.

The ability to exercise oversight over algorithmic systems must also not be subject to review by a trade tribunal, which prioritizes trade considerations over human and fundamental rights.[62] Scholars have noted that "[t]he contemporary lack of international standards and consensus on algorithmic governance increases a party's legal risk that an attempt to justify an inconsistent measure on ground of the general exceptions does not succeed."[63]

Looking to the adjudicatory history of the general public interest exceptions in the WTO provides evidence that trade tribunals would not prioritize public interest or human rights considerations. Referring to the General Agreement on Tariffs and Trade (GATT), the most recent analysis found that "in the WTO's 26 years of existence, there have been only two successful uses of the general exceptions of the GATT (Article XX) and the General Agreement on Trade in Services (GATS Article XIV) out of 48 attempts to defend domestic policies challenged as illegal under WTO rules."[64]

In addition, source codes are already protected by intellectual property law, including copyright, and, in some cases, patents, as well as trade secrets.[65] Intellectual property law operates a particular logic when to grant exclusive rights and in the case of copyright and patent protection it is subject to statutory limitations, and it must be published. Trade secret law is already undoing much of the balance struck because it is potentially unlimited and does not lead to the release of the protected subject-matter into the knowledge commons. The new bans on source code disclosures represent an additional layer of protection for algorithms in agreements affecting a broad swath of human activity in which hardly any other counterbalancing human, social, economic, or cultural rights are affirmed.[66] This is also why arguments alleging that corporations need these additional source code protections, or they will not deploy the latest technology in developing countries, fall flat.[67]

In addition, the exceptions contemplate, however insufficiently, only *known* risks of AI systems. As new risks and harms become known, it will be even more important for governments to maintain the power to regulate such algorithms to ensure that human and fundamental rights are upheld and that harms to society are reduced.

In combination with the myriad harms to European society detailed below, it is thus difficult to avoid the conclusion that there is no compelling justification for, and yet an overabundance of arguments against, including provisions barring governments from requiring source code disclosure in "trade" agreements.

There are other dangerous provisions in the digital trade rules under negotiation at the WTO, more of which will be referenced below.[68]

All of these provisions interact with each other as well as with existing trade rules, such as the GATS, the Agreement on Government Procurement, the Technical Barriers to Trade Agreement, and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) in the WTO, as well as other bilateral trade agreements and investment protection regimes. Thus, the potential impacts on European society and democracy of all these multiple overlapping provisions and agreements in an evolving digital and economic landscape go far beyond what is possible in this briefing and warrant further study.

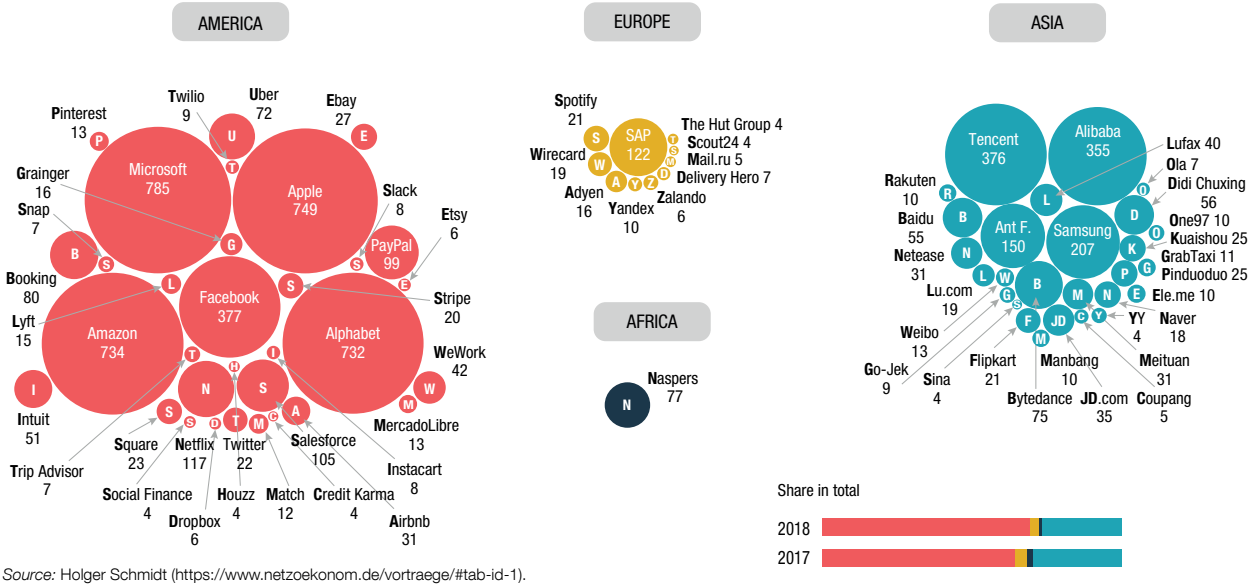
62 Irion, Kristina, "AI Regulation in the EU,' vzbv (2021).
63 Irion, 'Algorithms Off-limits?,' ACM (2022).
64 Rangel, 'WTO General Exceptions,' Public Citizen (2022). The two successful uses were U.S. – Shrimp and U.S. – Tuna-Dolphin.
65 Słok-Wódkowska and Mazur, 'Secrecy by Default,' *Journal of IntlEcon Law* (2022).
66 I am grateful to Kristina Irion for this insight.
67 In a 22 November 2022 conversation of the author with Aitor Montesa Lloreda, Head of the Digital Trade Sector in the Directorate General for Trade of the European Commission, he made this argument.
68 Deborah James, 'Digital Trade Rules: A Disastrous New Constitution for the Global Economy, by and for Big Tech,' *Rosa Luxemburg Foundation* (July 2020), https://www.rosalux.eu/en/article/1742.digital-trade-rules.html.

# 4.

# THE EU IS NOT POSITIONED TO BENEFIT FROM THESE RULES

There are two economic powerhouses that dominate digital trade economically, obviously the U.S. and China.[69] While the digital divide in terms of access to digitalization and the internet is narrowing, the economic digital divide with developing countries in Africa, Asia, and Latin America is expanding. But might be shocking to many that the digital economic divide is also expanding between Europe and the U.S./China. According to UNCTAD, the two countries also make up about 90 percent of the market capitalization of the world's largest digital platforms, and during the Covid-19 pandemic their profits and market capitalization values have surged tremendously.[70] In fact, only the German software company SAP registers as a major player in the platform landscape, visualized here by UNCTAD.

**Figure I.17. Geographical distribution of the main global platforms in the world, 2018**
(Market capitalization in billions of dollars)




*Source:* Holger Schmidt (https://www.netzoekonom.de/vortraege/#tab-id-1).

*Source: UNCTAD*[71]

In order to benefit from digitalization, UNCTAD argues that countries must engage in digital industrialization. Digital industrialization indicates the use of data and domestic digital infrastructures to create value in the digital economy. Building on ICT skills and connectivity, digital industrialization requires (local) data collection; (local) data storage; and (local) data servers to process big data sets into intelligence which can be used to operate AI.

69 UNCTAD, 'Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries,' United Nations (September 2019): xvi, https://unctad.org/system/files/official-document/der2019_en.pdf.
70 UNCTAD, 'Digital Economy Report 2021,' UN (2021).
71 See figure in UNCTAD, 'Digital Economy Report 2019,' UN (2019): 19.

As described below, in order to achieve the digital industrialization transformation that Europe is seeking, it will be necessary to engage in digital industrialization policies. The European Commission's Communication: "2030 Digital Compass: The European way for the Digital Decade"[72] evolves around the four cardinal points of expanding skills; ensuring secure and sustainable digital infrastructures; the digital transformation of business; and digitalisation of public services. For this Digital Strategy the EU is working on a series of new proposals, including a European Data Strategy[73], a European Industrial Strategy[74], the DSA[75], the DMA[76], a Cybersecurity Act[77], and the AI Act[78], among other regulatory projects.

At the same time, viewed through a rights-based lens, Europe is in a leadership position in terms of setting standards based on the European social model and the EU Charter of Fundamental Rights. European legislators are less afraid of regulating Big Tech than their American counterparts. Because of social dialogue, and the stronger role of trade unions and civil society in policy formulation, Europeans enjoy more digital rights and freedoms than citizens of other countries, including the U.S. and China. In these countries, it is predominantly the industry titans, and not ordinary people, who are "benefitting" from their country's market dominance.

The digital trade agenda being pursued by EU trade negotiators represents the commodification of workers and digital users for the benefit of (mostly) U.S.-based Big Tech corporations and is in fundamental contradiction to the recent efforts of European legislators and regulators.

72 European Commission, "Communication: 2030 Digital Compass: the European way for the Digital Decade," *European Commission* COM(2021) 118 final (March 2021), https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf; see also European Commission, 'A Europe fit for the digital age: Empowering people with a new generation of technologies,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.
73 European Commission, 'European data strategy,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
74 European Commission, 'European industrial strategy,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.
75 European Commission, 'The Digital Services Act: ensuring a safe and accountable online environment,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.
76 European Commission, 'The Digital Markets Act: ensuring fair and open digital markets,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
77 European Commission, 'The EU Cybersecurity Act,' EU website, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
78 European Commission, 'A European approach to artificial intelligence,' EU website, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

# 5.

# TEN WAYS THE EU'S DIGITAL TRADE RULES ARE NOT IN THE INTEREST OF EU CITIZENS, WORKERS, OR SMALL COMPANIES

*How would the EU's digital trade rules undermine...*

## 1- ... THE EU'S DIGITAL INDUSTRIALISATION AGENDA?

European leaders have embarked on a legislative and investment strategy towards a new industrial strategy for Europe that places digitalisation at its core.[79] The key objective is to catch up with China and the U.S. in the tech race, regulate Big Tech practices within the EU to prevent unfair competition, and reduce strategic dependence of raw materials, energy and the semiconductors needed for the digital industrialisation objectives. Europe's digital industrialisation strategy relies on improving access to data, developing technology and infrastructure, and appropriate regulation.[80]

Many of these steps are based on an emerging call for technological sovereignty. In particular, the EU's Commissioner for the internal market, Thierry Breton, has stressed the importance of the geopolitics of technology and technological sovereignty. "In this new geopolitical order, Europe acts like a strategist rather than just a market. It remains open, but on its own terms. It makes its own choices and draws up its own rules, and is not afraid of imposing them on its partners," Breton said in a 2021 speech.[81]

However, some of the EU's stated objectives clash with their digital trade strategy: first, with regards to the European commitment to a framework to allow businesses, particularly SMEs, to create, pool, and use data to improve products and compete internationally; second, to improve domestic or EU-wide digital infrastructures, such as cloud computing.

### European Data for Digital Industrialization

The EU has set forth the European Data Strategy[82] to create and pool data across strategic sectors, including both business to government (B2G) and business to business (B2B) data sharing. The idea is to create a common European data space for data to flow within the single market, to be available for innovation under GDPR and other European laws and with clear data governance mechanisms. As part of this strategy, the EU has approved the DGA[83] and the DA.[84] The DMA also provides significant data related rights to business users of larger platforms – like traders on Amazon. In some cases, public data will be available for reuse by public and private entities, in accordance with privacy and other governance rules. Business users of large platforms can get their data back from the platforms (under DMA), as also IoT users, like SMEs (under the DA), from data collectors. They can then employ provisions of DGA to develop data collaboratives to use their data in a manner that best suits them. In addition, there are incentives for private entities to provide data to the shared data spaces in the public interest.

79 European Commission, 'Communication: A New Industrial Strategy for Europe,' European Commission COM/2020/102 final (March 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593086905382&uri=CELEX%3A52020DC0102; European Commission, 'Communication: Updating the 2020 New Industrial Strategy: Building stronger Single Market for Europe's recovery,' European Commission COM/2021/350 final (May 2021), https://commission.europa.eu/system/files/2021-05/communication-industrial-strategy-update-2020_en.pdf.

80 European Commission, 'European industrial strategy,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.

81 Luca Bertuzzi, 'Mastery of technology is central to the 'new geopolitical order', Breton says,' *Euractiv* (July 2021), https://www.euractiv.com/section/industrial-strategy/news/mastery-of-technology-is-central-to-the-new-geopolitical-order-breton-says/.

82 European Commission, 'European data strategy,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

83 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act),' European Commission COM/2020/767 final (November 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767.

84 European Commission, 'Data Act,' EU website, https://digital-strategy.ec.europa.eu/en/policies/data-act

In the case of the DA, there are also means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency, such as floods and wildfires, or to implement a legal mandate if data are not otherwise available. The draft DA also gives users of IoT devices rights to access their data that may be collected by various platforms and apps, and to share it.

However, a great amount of data that is generated in Europe is held by foreign-based companies that should also be required to share data for the benefit of Europeans.[85] European drivers and riders produce data for Uber, which Uber then utilizes to extract further profit from European society, all the while using European public investments in roads and infrastructure. European public weather data is used by the global insurance industry to capitalize on predicting massive weather events. European consumers make purchasing choices on Amazon, which the U.S.-based corporation then uses to downgrade European SMEs and highlight its own products. In all these cases, European data is captured by transnational corporations (TNCs), many foreign, for private, mostly foreign, profit.[86]

Under the DGA, these TNCs would have access to European public data. At the same time, they do not appear to be obligated to share data with European SMEs or the public sphere. Digital trade rules that require states to allow data to be transferred overseas and prohibit governments from being able to require a set of the data to be held locally would constrain Europe's ability to require reciprocity in data sharing. The large troves of data required to scale digital industrialization would be compromised as a result.

## European Digital Infrastructures

Effectively managing large data sets for digital industrialization requires the creation of digital infrastructures, in particular data centres used for cloud computing. That's why Europe's industrial strategy identifies the importance of promoting data infrastructure including cloud computing as a necessary prerequisite. But U.S.-based companies Amazon Web Services, Microsoft Azure, and Google Cloud, together dominate 65 percent of the global cloud market.[87] A recent study noted that although European cloud hosting providers have seen revenues rise by 167 percent since 2017, their market share has plummeted from 27 percent to 15 percent within the same period, as the three above U.S.-based companies now control nearly 72 percent of the European cloud storage market.[88]

Rather than be dependent on American-domiciled data centres, the French government has promoted a local data-centre infrastructure. France has mandated that all data from public administrations has to be considered as archives and therefore stored and processed in France.[89] In May 2021, France mandated that cloud services providers must: "fulfil the security requirements associated with the 'SecNumCloud' technical reference; locate the infrastructures and operate the systems in Europe; and ensure the operational and commercial support of the offer by a European entity, owned by European actors."[90]

As part of its NextGenerationEU plan,[91] the EU is enabling a European cloud, Gaia-X, to address growing alarm over the dependence of domestic firms, government services, and even security services on foreign cloud hosts.[92] However, despite a governance structure that is tied to European firms, the leading U.S. cloud providers are already an inseparable part of Gaia-X.[93]

85 The current or proposed provisions of the DMA and DA (in conjunction with DGA) are useful but, according to some experts on digital industrialization, not adequate. More stress should be given on collective data and collective agency that can usefully share and use it. See Parminder Jeet Singh and Anita Gurumurthy, 'A Primer on Data and Economic Justice,' *Global Partnership on Artificial Intelligence* (November 2022), https://gpai.ai/projects/data-governance/primer-on-data-and-economic-justice.pdf.

86 Rosie Collington, 'Digital Public Assets: Rethinking value and ownership of public sector data in the platform age,' Common Wealth (November 2019), https://www.researchgate.net/publication/337110612_Digital_Public_Assets_Rethinking_value_access_and_control_of_public_sector_data_in_the_platform_age.

87 Felix Richter, 'Top Cloud Market Share Leaders: AWS, Microsoft, Google Lead Q2 2022,' *Statista* (December 2022), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

88 Will McCurdy, 'European cloud market is being dominated by three big players,' TechRadar (September 2022), https://www.techradar.com/news/european-cloud-market-is-being-dominated-by-three-big-players.

89 Government of the French Republic, Stratégie Nationale Pour Le Cloud (May 2021), https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/

90 Matteo Quartieri, 'France: The new national cloud strategy - data transfers and localisation implications,' DataGuidance (May 2021), https://www.dataguidance.com/opinion/france-new-national-cloud-strategy-data-transfers.

91 'State of the Union Address by President von der Leyen at the European Parliament Plenary,' European Commission (September 2020), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

92 Janosch Delcker, 'Germany's plan to control its own data,' *Politico EU* (September 2019), https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/.

93 Louis Westendarp and Peter O'Brien, 'Gaia-X board member blames lobbying for project's gridlock,' *Politico EU* (July 2022), https://www.politico.eu/article/eu-lobbying-cloud-project-gaia-x-board-member-says-cloud-project-must-neuter-lobbies-role-to-get-on-track/.

Germany has also tabled proposals for similar restrictions on sovereignty requirements on the European cybersecurity cloud certification scheme, which are also supported by France, Italy and Spain.[94] But they are opposed by a number of European countries as well as U.S.-based Big Tech cloud services providers. Business lobbies primarily representing U.S.-based Big Tech oppose digital industrialization strategies and have long complained about these policies, which are meant to promote digital industrial capacities in Europe.[95]

But the EU's digital trade rules against data localisation proscribe states from: being able to require 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 the Party; requiring the localisation of data in the Party's territory for storage or processing; and making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.[96] If the EU could not ensure that EU-based data infrastructure is utilized, then cloud carriers such as Amazon, Google, and Microsoft will pursue their data storage and processing needs in cheaper data havens, not in Europe.

Some researchers have simply advocated an expansion of digital trade agreements to improve European access to foreign markets, without reflecting on whether foreign access to the European market in a strategic sector like data infrastructure could compromise digital industrialization.[97] If the European cloud market is dominated by U.S.-based Big Tech, then it is not clear how gaining additional market access for those companies to third countries' data could benefit Europeans.

These are complex issues with implications for who benefits economically from data, as well as European political dependence on foreign firms. They must be debated and decided democratically. They should not be determined by the market access commitments in trade agreements, nor should the debates be overly influenced by the economic lobby power of foreign firms, or think tanks funded by foreign firms.[98]

The EU's digital trade policies thus appear in fundamental contradiction to the recent emergence of widespread concern about the dominance of U.S.-domiciled Big Tech behemoths, their control over and abuse of European data in ways that harm European society, and the general agreement about the need to engage in mitigation strategies that would strengthen more widespread European economic benefits of digitalization.

94 Luca Bertuzzi, 'Germany calls for political discussion on EU's cloud certification scheme,' Euractiv (September 2022), https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/.

95 BusinessEurope, 'Free Flow of Data is at the essence of a true European Digital Single Market,' Confederation of European Business public letter (November 2016), https://www.businesseurope.eu/sites/buseur/files/media/public_letters/imco/2016-11-29_ffd_joint_statement.pdf.

96 Chapter XX Article X.4 in EU-New Zealand FTA, Also Title III Article 201 in EU-UK TCA.

97 Georgios Petropoulos et al, 'Data flows, artificial intelligence and international trade: impacts and prospects for the value chains of the future,' European Parliament analysis requested by the INTA committee (November 2020), https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2020)653617.

98 See as example: Nigel Cory, "Sovereignty Requirements' in France—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners,' Information Technology and Innovation Foundation (ITIF) (December 2021), https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi/. A list of ITIF funders at https://itif.org/our-supporters/ includes Amazon, Meta, Microsoft, Uber, Visa, and Walmart among others.

## 2- ... THE EU'S ABILITY TO TAX BIG TECH?

Digital firms have seen their profits soar over the last few years as a result of a sharp increase in cross-border digital activities as a result of the Covid-19 pandemic. Yet the taxes they pay remain extremely low, including in Europe.[99] Low taxes by Big Tech companies are the result of tax evasion and avoidance and excessive tax incentives by some governments, but also the fact that the current tax system is not fit for digital transactions.[100] This is especially the case in the digital space where the level of value addition can easily be moved across different parts of the value chain which may be located in different territories. A company like Uber for instance can easily shift "highest value creation" from the country of its operation to a tax haven like Ireland from where the backend software and analytics are shown to be provided.[101] Big Tech firms rely heavily on tax havens to shift profits, avoid taxes, store wealth, and circumvent regulation.[102] In 2019, Fair Tax Mark reported that Google, Facebook, Apple, Microsoft, Netflix and Amazon together evaded over $100 billion in taxes from 2011-2020.[103]

Big Tech deploys a two-pronged approach to maintain this beneficial situation. They lobby against modifications to the tax system. In parallel, they promote digital trade rules that limit states' ability to tax them.

In 2016, the EU had already identified the unfair taxation of the digital economy. First, the Commission accused Apple[104] and Amazon[105], of illegal tax benefits. In 2018, it launched a Communication proposing to restructure the taxation system for the digital economy,[106] a project that was later abandoned after pressure from the US and big tech companies.[107]

The global tax agreement reached at the OECD in 2021 is currently the only deal that might help to ensure that digital firms pay a fairer share in taxes,[108] although it has been criticized for not doing enough to restore tax redistribution towards countries where digital giants actually operate.[109] And its adoption, especially by the U.S., is quite uncertain.[110]

This novel agreement might be undermined by numerous different provisions in digital trade agreements that seek to constrain states' ability to tax electronic trade.[111] A group of experts conducted a thorough investigation[112] concluding that digital trade rules would impede taxation in developing countries. Such a study has yet to be conducted on European tax policy. Nonetheless, an initial analysis indicates that the EU's efforts to tax Big Tech could be contradicted by its own digital trade policies.

### Ban on customs duties on electronic transmissions

Nearly all EU trade agreements with digital provisions include a ban on customs duties on electronic transmissions (ETs). This means that while importers of products such as cars, watches, and agricultural goods are subject to duties, or trade taxes, if the same good is electronic – as in the case of books, movies, or music – states are prohibited from

99 In the EU, cross-border digital activities were subjected to an average tax rate of only 9.5%, according to a 2017 study. European Commission, 'Commission Staff Working Document Impact Assessment, Accompanying the document 'Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence,' and 'Proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services," European Commission SWD(2018) 81 final/2 (March 2018): 18, https://taxation-customs.ec.europa.eu/document/download/89deda55-f8a7-40f1-a767-46d58f500518_en?filename=fair_taxation_digital_economy_ia_21032018.pdf.

100 European Commission, 'Commission Staff Working Document Impact Assessment,' European Commission SWD (2018) 81 final/2 (2018).

101 Scilla Alecci, 'Uber shifted scrutiny to drivers as it dodged tens of millions in taxes: Executives agreed to share driver data to 'contain' a tax audit and deflect from the tech giant's use of European and Caribbean tax havens, new leak shows,' *International Consortium of Investigative Journalists* (July 2022), https://www.icij.org/investigations/uber-files/uber-tax-havens-dodge-drivers/. See also Brian O'Keefe and Marty Jones, 'How Uber plays the tax shell game,' *Fortune* (October 2015), https://fortune.com/2015/10/22/uber-tax-shell/.

102 Rodrigo Fernandez et al, 'Engineering Digital Monopolies: The financialisation of Big Tech,' Centre for Research on Multinational Corporations (SOMO) (December 2020), https://www.somo.nl/the-financialisation-of-big-tech/.

103 Fair Tax, 'Tax gap of Silicon Six over $100 billion so far this decade,' Fair Tax press release (December 2019), https://fairtaxmark.net/tax-gap-of-silicon-six-over-100-billion-so-far-this-decade/.

104 European Commission, 'Ireland granted undue tax benefits to Apple,' European Commission press release (August 2016), https://ec.europa.eu/commission/presscorner/detail/en/ac_16_3727.

105 European Commission, 'State aid: Commission finds Luxembourg gave illegal tax benefits to Amazon worth around €250 million,' *European Commission* press release (October 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3701.

106 European Commission, 'Fair Taxation of the Digital Economy,' EU website, https://taxation-customs.ec.europa.eu/fair-taxation-digital-economy_en.

107 Mark Scott and Emily Birnbaum, 'How Washington and Big Tech won the global tax fight,' Politico EU (June 2021), https://www.politico.eu/article/washington-big-tech-tax-talks-oecd/.

108 See the 'Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy – 8 October 2021,' OECD/G20 Base Erosion and Project Shifting Project (October 2021), https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm.

109 'South Centre Comments on the 'Progress Report on the Administration and Tax Certainty Aspects of Amount A of Pillar One,'' *South Centre* submission to the OECD TFDE on the Progress Report on the Administration and Tax Certainty Aspects of Amount A of Pillar One (November 2022), https://www.southcentre.int/south-centre-comments-on-progress-report-on-administration-and-tax-certainty-aspects-of-amount-a-11-november-2022/.

110 Mary McDougall, 'Biden Tax proposals fall short of OECD standards for minimum rate,' Financial Times (August 2022), https://www.ft.com/content/ff0c15b7-2e34-469f-8c5e-9168bbb30c51.

111 Deborah James, 'Anti-development Impacts of Tax-Related Provisions in Proposed Rules on Digital Trade in the WTO,' *Development* 62 (2019): 58-65, https://doi.org/10.1057/s41301-019-00205-4.

112 Jane Kelsey et al, 'How 'Digital Trade' Rules Would Impede Taxation of the Digitalised Economy in the Global South,' *Third World Network* (August 2020), https://twn.my/title2/latestwto/general/News/Digital%20Tax.pdf.

imposing duties. This ban is prejudicial towards importers and retailers of analogue versions of the same goods, which are more likely to be local businesses rather than digital behemoths such as Amazon, Netflix, or Apple.[113]

The EU has always been a net importer of ET products (as identified in the WTO Note, 2016).[114] Over time, imports of the EU are growing much faster than its exports, with net imports of these products rising from $2.2 billion in 2020 to $4.4. billion in 2021. The net imports of video games increased from $3.5 billion in 2020 to $5.3 billion in 2021. The average bound duties in the EU on these ET products are 6.5 percent which can be instrumental in regulating imports of these products in many EU countries.[115]

A key argument used by defenders of this ban, or moratorium, is that it benefits EU digital export SMEs. But large U.S.-based corporations, including Apple (music), Netflix (movies), and Amazon (books) benefit from the moratorium far more than SMEs in the EU, which are far more likely to be responsible for normal customs and other taxes that are part of doing business.

This provision has become an extremely controversial issue at the WTO, where a moratorium on such duties has been renewed every Ministerial since 1998. But the evidence that this Big Tech tax holiday is hurting developing countries' growth prospects is mounting, and at the 12th Ministerial Conference (MC12) in June of 2022 they pushed for it to expire. After heavy pressure from Big Tech, in the end the moratorium was renewed for another year, but the battle will continue on to the next Ministerial. Starving poor countries of revenues needed to fund their own development to give a tax break to Amazon is not in the interests of the European public.

There is also some effort to expand the moratorium on taxes on electronic commerce to include taxes on digital services. But many European countries have implemented digital services taxes (DSTs). According to the Tax Foundation, about half of all European countries have either announced, proposed, or implemented a digital services tax in recent years.[116] Because the most profitable companies that would be affected by the taxes are U.S.-based, the U.S. government has considered them discriminatory, although they are applied across the board, and has threatened retaliatory tariffs. In October 2021, Austria, France, Italy, Spain, the UK, agreed to remove DSTs and the U.S. agreed to remove retaliatory tariff threats, as the new Pillar One rules of the OECD agreement are implemented.[117] But if the U.S., or other trade partners, fail to implement the Pillar One rules, or if they do not result in the increased revenue anticipated, European countries may well want to maintain the ability to tax digital services.

## Bans on data localisation

But it is not just direct taxes that Big Tech seeks to prevent through trade agreements. A provision banning governments from being able to require a copy of data to be held locally makes it more difficult for governments to assess corporate profit taxes, an issue of serious concern to legislators and regulators. Many countries require the data of foreign firms to be stored locally so that tax authorities have the ability to review the data in case of any audit or requirement for review. For example, Denmark's Book Keeping Act requires companies to store accounting data in Denmark for five years.[118]

Tax havens are increasingly used by Big Tech as "data havens" to prevent government access to data that could have tax implications otherwise.[119] Data localisation bans in digital trade agreements encourages this practice.

113 Richard Kozul-Wright and Rashmi Banga, 'Moratorium on Electronic Transmissions: Fiscal Implications and the Way Forward,' *UNCTAD* Research Paper No. 47 (June 2020), https://unctad.org/system/files/official-document/ser-rp-2020d6_en.pdf.

114 WTO General Council, 'Fiscal implications of the customs moratorium on electronic transmissions: the case of digitisable goods (Doc # 16-6961),' WTO JOB/GC/114 (December 2016).

115 Calculations available from the author, based on COMTRADE, World Integrated Trade Solutions, UNCTAD and World Bank data.

116 "Austria, France, Hungary, Italy, Poland, Portugal, Spain, Turkey, and the United Kingdom have implemented a digital services tax. Belgium, the Czech Republic, Denmark, and Slovakia have published proposals to enact a digital services tax, and Latvia, Norway, and Slovenia have either officially announced or shown intentions to implement a digital tax." Daniel Bunn and Elke Asen, 'What European Countries Are Doing about Digital Services Taxes,' *Tax Foundation* (August 2022), https://taxfoundation.org/digital-tax-europe-2022/.

117 'Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect,' U.S. Department of the Treasury press release (October 2021), https://home.treasury.gov/news/press-releases/jy0419.

118 Under special circumstances, the Danish Commerce and Companies Agency may grant companies permission to preserve accounting records abroad. However, the practice has proven quite restrictive, and permission is seldom granted. Matthias Bauer et al, 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States,' *European Centre for International Political Economy* Policy Brief (March 2016), https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

119 Sofia Scasserra and Adriana Foronda, 'Banking on data: How the world's tax havens became the data centres for the digital economy,' *Transnational Institute* (November 2022), https://www.tni.org/en/publication/banking-on-data.

The EU's country-by-country reporting directive aimed at enhancing public scrutiny of corporate income taxes should improve reporting,[120] but digital trade rules run counter to this objective. Margrethe Vestager has noted, "even if we get the perfect implementation of this possible deal, I still think there will still be a job to do to look for those who spend energy, creativity, lawyers' fees to escape paying their taxes."[121]

Researchers have identified many other digital trade provisions that could limit the ability of states to tax Big Tech.[122] There are also exceptions in the tax provisions which provide more flexibility or carve-outs. However, these often draw on outdated WTO exceptions that are not fit for purpose in the digital age, such as in the EU-NZ FTA, or are impossibly complex.[123]

Big Tech should not be able to obtain further provisions in "trade" agreements that help them to evade fair taxation.

## 3- ... EU'S AGENCIES' POWER TO REGULATE BIG TECH?

Europe is also betting that it can regain a leading position by setting global standards for the Internet. As set forth in the EU's Digital Strategy, this includes efforts to protect people from cyber threats (hacking, ransomware, identity theft); to ensure AI is developed in ways that respect people's rights and earn their trust; to increase access to high-quality data while ensuring that personal and sensitive data is safeguarded; to enable a vibrant community of innovative and fast-growing start-ups and SMEs to access finance and to expand; and many other people-centred goals.[124]

Emerging concerns demonstrate that preserving policy space for regulation is far more crucial to re-establishing European leadership, ensuring widespread benefits from digitalization, and guaranteeing European fundamental rights in the digital sphere. The digital trade rules are broad and all-encompassing. Public interest regulation would be subject to challenges with only the narrow window of limited exceptions for public interest regulation available as a defence. Future-proofing the ability to regulate according to evolving political and economic landscapes thus far outweighs any claims of alleged benefits of digital trade rules put forward by Big Tech. Permanent, binding proposals for treaties which promote U.S.-based Big Tech wish lists to hamstring European regulation is obviously not the path forward, given the emerging political consensus in the EU on digital industrialization, and all of the concerns outlined below.

Myriad aspects of the urgent need to regulate of Big Tech would be affected by the digital trade rules. This section focuses on two aspects: financial regulation and cybersecurity.

### Regulating the financial sector

Decisions such as who will get a loan for a house or car purchase or who will be awarded insurance based on credit risks are increasingly made by data and algorithms. But algorithmic systems are prone to discrimination.[125] If a machine "learns" that people with certain types of names, or refugee status, or current address, are a higher risk, those algorithms could indicate a higher interest rate than would have been assigned based on legal criteria such as income level and credit history. There are countless reasons why a government needs to be able to have access to source code in order to regulate financial transactions to ensure fundamental rights are not violated.

Aside from fairness in regulating the financial sector, there is the key issue of financial stability. High frequency trading and the growing automation of stock markets operations pose enormous risks in terms of financial stability, due to intensifying volatility, ripple effects, uncertainty, and errant algorithms.[126] And similar arguments are being made with regards to cryptocurrencies and ransomware[127] and money laundering, according to the European Systemic Risk

120 'Directive (EU) 2021/2101 of the European Parliament and of the Council of 24 November 2021 amending Directive 2013/34/EU as regards disclosure of income tax information by certain undertakings and branches (Text with EEA relevance),' European Parliament PE/74/2021/INIT (November 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.429.01.0001.01.ENG&toc=OJ%3AL%3A2021%3A429%3ATOC.
121 Interview with Molly Wood and Stephanie Hughes, 'Big Tech dodged one tax bullet, but another one is coming,' *Marketplace Radio* (July 2021), https://www.marketplace.org/shows/marketplace-tech/big-tech-dodged-one-tax-bullet-but-another-one-is-coming/.
122 Kelsey et al, 'How 'Digital Trade' Rules Would Impede,' TWN (2020).
123 Ibid: 41-44.
124 European Commission, "Shaping Europe's digital future," *European Commission* fact sheet FS/20/278 (February 2020), https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278.
125 Adair Morse and Karen Pence, 'Technological Innovation and Discrimination in Household Finance,' *National Bureau of Economic Research* working paper no. 26739 (February 2020), https://www.nber.org/system/files/working_papers/w26739/w26739.pdf.
126 Elvis Picardo, '4 Big Risks of Algorithmic High-Frequency Trading,' Investopedia (January 2022), https://www.investopedia.com/articles/markets/012716/four-big-risks-algorithmic-highfrequency-trading.asp.
127 World Economic Forum, "The Global Risks Report 2022: 17th Edition," World Economic Forum (January 2022), https://wef.ch/risks22.

Board (ESRB),[128] leading the European Council to pass the Markets in Crypto-Assets (MiCA) regulation in October 2022.[129] Decisions in the financial sector are increasingly determined by algorithms which must be subject to regulatory oversight and public scrutiny. The financial sector is subject to an exception for prudential measures but it is quite contentious.[130]

Trade provisions which bar governments from requiring disclosure of source code in order to ascertain the security of the financial sector would preclude the regulatory oversight necessary to guarantee financial security in a situation where algorithmic trading captures an expanding share of financial markets and has implications for financial stability.

## Electronic Authentication

The rules would also bar states from being able to set the authentication method of an online transaction. According to Chapter X.9 on Electronic Authentication of the EU-NZ agreement, "No Party shall adopt or maintain measures that would: prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for that transaction." The basic implication of this rule is that government could not require a higher level of security.[131] However, history is full of examples of states failing to regulate security in financial transactions and paying the price.

It has been through regulation that financial services companies and other firms have improved the security of their transactions. Two factor authentication (TFA) is becoming the global standard for financial and other high-risk transactions. The EU's Second Payment Services Directive (PSD2) includes a mandate for Strong Customer Authentication (SCA),[132] the key enabler of which is TFA. But this could be subject to challenge by a foreign service provider given their "right" to determine the electronic authentication methods under trade agreements. Of course, electronic authentication is also important for a broader range of issues, including the IoT.

## Regulating Cybersecurity in the Internet of Things (IoT)

The number of products that consumers use on a daily basis that are connected to the internet is growing exponentially. The IoT market for digitally connected devices is an emerging concern for cybersecurity specialists, as IoT devices have been the subject of regular cyberattacks and data leakages. A European Commission impact assessment report estimated that the annual costs of data breaches exceed 10 billion euros and the annual costs of malicious attempts to disrupt internet traffic likely exceed 65 billion euros.[133]

In addition to costs and the safety and security of data, this is also a key issue of human health and safety. Networked automobiles could be hacked and driven dangerously; hacking of medical devices such as pacemakers could allow bad actors to damage human health; the hacking of baby monitors could endanger children. Given the poor state of cybersecurity regulation worldwide, European governments are increasing cybersecurity legislation on IoT devices in order to protect sensitive consumer (including financial) data and safety.

On 22 March 2022, the European Commission adopted two new proposals for a Cybersecurity Regulation[134] and an Information Security Regulation[135] which updated the existing framework of 2019. These regulations, which are still undergoing legislative procedures, build on the EU Security Union Strategy and the EU's Cybersecurity Strategy for the Digital Decade.[136]

128 Jack Schickler, 'Crypto Popularity Could Pose Stability Risk, EU Watchdog Warns, as It Ponders New Powers,' *CoinDesk* (March 2022), https://www.coindesk.com/policy/2022/03/31/crypto-popularity-could-pose-stability-risk-eu-watchdog-warns-as-it-ponders-new-powers/.
129 Issam Hallak, 'Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets,' in 'A Europe Fit for the Digital Age,' Legislative Train (December 2022), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1.
130 Kelsey et al, 'How 'Digital Trade' Rules Would Impede,' TWN (August 2020): 48.
131 Sanya Reid Smith, 'Electronic Authentication: Some Implications,' *Third World Network* (August 2018), https://ourworldisnotforsale.net/2018/esignatures2018-9.pdf.
132 European Banking Authority, 'Question on delegation of 2-Factor Authentication (2FA) to PISP, AISP or other third party,' EBA Question ID 2020_5643 and Legal Act Directive 2015/2366/EU (PSD2), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5643.
133 European Commission, 'Commission Staff Working Document Impact Assessment Report Accompanying the document: Commission Delegated Regulation supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive,' *European Commission* SWD(2021) 302 final (October 2021), https://single-market-economy.ec.europa.eu/system/files/2021-10/SWD%282021%29%20302_EN_impact_assessment_part1_v3.pdf.
134 European Commission Directorate-General for Informatics, 'Proposal for Cybersecurity Regulation,' European Commission Proposal for a Regulation (March 2022), https://ec.europa.eu/info/publications/proposal-cybersecurity-regulation_en.
135 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union,' European Commission COM(2022) 119 final (March 2022), https://ec.europa.eu/info/files/proposal-regulation-information-security-institutions-bodies-offices-and-agencies-union_en.
136 Sarah O'Brien and Cynthia O'Donoghue, 'European Commission adopts two proposals for cybersecurity and information security regulations,' ReedSmith Technology Law Dispatch (April 2022), https://www.technologylawdispatch.com/2022/04/privacy-data-protection/european-commission-adopts-two-proposals-for-cybersecurity-and-information-security-regulations/.

In September 2022, the European Commission proposed new regulations specifically on smart devices, the Cyber Resilience Act (CRA).[137] The new rules will complement the existing Network and Information Systems (NIS Directive),[138] the NIS 2 Directive[139] (covering cloud providers and software as a service), and the EU Cybersecurity Act.[140]

Cybersecurity regulation on IoT will require standards such as TFA, and the disclosure of source code to relevant authorities to evaluate high-risk algorithms and cybersecurity measures. But the provisions of "digital trade" rules promoted by the EU would bar states from being able to require necessary disclosure of source code, even subject to certain exceptions.

These constraints are unacceptable given past practice and current needs for strengthening oversight of cybersecurity in the public interest. As discussed above, the exceptions in the source code disclosure provisions – including in the most recent EU-NZ FTA – still far short of the enormity of the urgent need for more public oversight.

Some pro-corporate advocates argue that trade provisions can be used to ensure that cybersecurity rules do not become protectionist, in terms of favouring international standards which are not trade-restrictive.[141] However, Europeans have stated clear goals to set standards which are higher than those extant internationally at this time.[142] The idea that states should be constrained by trade agreements against the adoption of higher standards makes no sense in the face of evolving cybersecurity threats and the ongoing need for higher security standards.

Rather, cybersecurity is a fundamental issue of public safety and security and fundamental rights. Standards should be set through democratic channels, with public debate, based on a high level of skilled technical inputs. The economic interest of foreign firms, such as Big Tech, should not be a consideration given the gravity of the issues, and those same firms' history of abusive data practices and cybersecurity leaks.

## 4- ... EU'S PUBLIC SERVICES?

Quality, accessible public services are a cornerstone of European life and a key underpinning of the social contract that results in the higher quality of life and longevity experienced by European residents. But public services could be negatively impacted by proposed Big Tech digital trade rules. The potential impact on taxation and government revenue, which is essential to maintain affordable, quality public services, is just one such problem. Human rights organizations have raised concerns about the overreliance on algorithmic decision-making to determine social and economic rights such as access to social benefits and other public services,[143] which requires AI to be subject to proper oversight.

The proposed rules could lead to the further privatization of public services, and to the resulting job losses and erosion of workers' rights. Digitalization of public services often involves public-private partnerships with Big Tech corporations, which facilitate the privatization of jobs. Privatization has been shown to reduce the number of quality of jobs, as firms compete by lowering wages and benefits and skim a profit from the government payments.[144]

137 European Commission, 'EU Cyber Resilience Act: New EU cybersecurity rules ensure safer hardware and software,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
138 European Commission, 'NIS Directive,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/nis-directive.
139 European Commission, 'Commission welcomes political agreement on new rules on cybersecurity of network and information systems,' European Commission press release (May 2022), https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985.
140 European Commission, 'The EU Cybersecurity Act,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
141 Joshua P. Meltzer and Cameron F. Kerry, 'Cybersecurity and digital trade: Getting it right,' Brookings report (September 2019), https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/.
142 See European Commission, 'Secure solutions for the Internet of Things,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/secure-internet-things.
143 See 'on the digital welfare state': Phillip Alston, 'Report of the Special Rapporteur on Extreme Poverty and Human Rights,' UN Human Rights Council A/74/48037 (October 2019), https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx; Lina Dencik and Anne Kaun, 'Datafication and the Welfare State: An Introduction,' *Global Perspectives* 1, no. 1 (2020), https://www.diva-portal.org/smash/get/diva2:1448242/FULLTEXT02.pdf; Human Rights Watch, 'UN: Protect Rights in Welfare Systems' Tech Overhaul,' HRW news release (October 2019), https://www.hrw.org/news/2019/10/17/un-protect-rights-welfare-systems-tech-overhaul.
144 Christina J. Colclough, 'Reshaping the Digitization of Public Services,' *New England Journal of Public Policy 34*, no. 1 (October 2022), https://scholarworks.umb.edu/nejpp/vol34/iss1/9.

At the same time, privatization removes a wide swath of aspects of those services from public oversight. For example, digitalization in health care involves "tele-health" but also the digitalization of record-keeping, of diagnostics, of decisions around personnel and allocation of resources, and of algorithms determining insurance coverage - all of which would be subject to the new digital trade rules and thereby less subject to regulation.[145]

Maintaining a strong public services sector in Europe will require strengthening algorithmic accountability and up-skilling digital knowledge among public workers. It will also require the use of large data sets by the public sector to improve education, health, transportation, water and electricity distribution, and other public services. It will also require that public services maintain the right to access and control the data produced through any partnerships with private companies. These goals will not be possible to achieve if Big Tech succeeds in barring source code disclosure and maintaining data collection in the private sphere.

### Smart Cities

"Smart Cities" are digitally connected cities that use a lot of data collection to help with city planning, including in public services. But citizen movements in some cities have also pushed back against the extraction of their data for private profit. In Europe, Barcelona has broken away from business as usual. For a long time, it has been a pioneer among Smart Cities. Sensors on light posts dim when people are not around, saving the city millions of dollars on electricity. Water meters sense the moisture needed in public parks, saving tens of millions in water costs.[146]

But over time, citizens rejected how the data they generated from public services was being privatized and held by corporations though public-private partnerships. Now, the city spearheads the data for the public good movement through the lens of data autonomy and the shift of data governance. The low-hanging fruit was procurement: the city now insists on data disclosure in its contracts with tech companies. Francesca Bria, then Barcelona's Chief Technology and Digital Innovation Officer, said "we are introducing clauses into contracts, like data sovereignty and public ownership of data."[147] Through the European Decode Project (DEcentralised Citizen-owned Data Ecosystems)[148] piloted by innovators Barcelona and Amsterdam, cities are rethinking their future, adapting the technology and data infrastructure around its citizens rather than starting with the tech.

This data can be generated as a public resource as part of the operation of public services. But if the data collection of the public service, or the provision of the service itself, is privatized, then so is the data. In order to obtain the data to improve public services and save jurisdictions valuable tax dollars, the data would have to be transferred from the private operator to the public.

Even though most cities in Europe are not yet taking steps to ensure data sovereignty and public ownership of data, if they would, under the proposed EU digital trade rules barring states from requiring the localisation of data in the Party's territory for storage or processing, the required disclosure from companies could be challenged under trade agreements.

## 5- ... EU'S CITIZENS PRIVACY AND DATA PROTECTION RIGHTS?

The landmark legislation of the GDPR published in 2016 set the global standard for the fundamental rights of data privacy and data protection. Non-Europeans have criticized GDPR as a key trade barrier.[149] Since that time, the urgent need to safeguard the human right to privacy and the fundamental right of data protection under the metastasizing effects of surveillance capitalism have only increased.[150]

And yet the proposals of the EU on digital trade in bilateral or regional agreements, and at the WTO, maintain provisions guaranteeing the rights of corporations to transfer data, including personal data, across borders.

145 There is a carveout, including in Article 1 of the EU-NZ FTA for information held or processed by or on behalf of a party, including measures relating to its collection. The boundaries are unclear, especially when private firms are collecting and storing the data and can relocate and use it.
146 Laura Adler, 'How Smart City Barcelona Brought the Internet of Things to Life,' Data-Smart City Solutions (February 2016), https://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789.
147 Thomas Graham, 'Barcelona is leading the fightback against smart city surveillance,' Wired (May 2018), https://www.wired.co.uk/article/barcelona-decidim-ada-colau-francesca-bria-decode.
148 See the DECODE project here: https://decodeproject.eu/what-decode.
149 Philip Thompson, 'The International Trade barrier Index 2021,' Tholos Foundation (2021), https://atr-tbi19.s3.amazonaws.com/TBI_FullReport_2021_FINAL.pdf
150 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs: January 2019).

The European Parliament was the first to raise the alarm in Europe about the need to exclude personal data protection from free trade agreements.[151] Since 2018, the EU has tried to balance maintaining unrestricted FFOD, with some protection of personal data to comply with GDPR legislation. Recent trade agreements, like the ones with the UK and New Zealand, include a clause that aims to safeguard the protection of personal data and privacy. However, there are serious doubts that the "safeguards" included will indeed protect personal privacy.

Subsequent to the publication of the EU-UK TCA, the European Data Protection Supervisor (EDPS) stated that he "regrets that the TCA fails to faithfully take over the EU's horizontal provisions for cross-border data flows and for personal data protection. Such provisions, which the European Commission has repeatedly stated as non-negotiable, allow the EU to include measures to facilitate cross-border data flows in trade agreements while preserving individuals' fundamental rights to data protection and privacy. Thus, in amending these horizontal provisions, the TCA creates legal uncertainty about the EU's position on the protection of personal data in the context of trade agreements and risks creating friction with the EU data protection legal framework."[152]

Scholars investigating whether the GDPR can apply under the provisions of cross-border data transfers in digital trade agreements have concluded that "trade law should not move ahead in setting the rules for cross-border trade in the era of big data and AI without recognizing the members' responsibility to take appropriate measures that would ensure that AI and overall data governance are fully accountable to domestic human rights frameworks."[153]

Civil society organizations have reiterated calls that "[i]f 'cross-border data flows' rules are part of the future WTO agreement, existing safeguards must ensure that people's privacy and data protection rights always have priority over data flow rules so that the digital economy can thrive and people can trust that fundamental rights law is respected. If these conditions cannot be met, countries must exclude or not commit to rules on cross-border data flows in the negotiations and in any final deal. Endorsing other binding international rules – notably the Council of Europe's Convention 108+ for the Protection of Individuals with Regard to the Processing of Personal Data[154] – will be more balanced. To date, 55 countries have become parties to Convention 108+ already."[155]

It is interesting to note that while EU has understood the importance of protecting personal data and has put in place policies to protect it, the digital revolution is revealing the importance of protecting non-personal data. One of the reasons for protecting non-personal data is because the latest research[156] shows that by using reverse engineering and machine learning non-identifiable data can re-identify individuals i.e., non-personal data can be converted into personal data. The research demonstrates for the first time how easily and accurately this can be done - even with incomplete datasets. In the research, 99.98 per cent of Americans were correctly re-identified in any available "anonymized" dataset. Thus, if restrictions on cross-border flow of personal data are allowed and digital rules are made flexible with respect to "personal" data to protect privacy and for national security reasons then the same flexibilities are required for protecting the non-personal data.

## Adequacy decisions

The EU allows free flow of personal data to third countries with whom there is an adequacy decision which guarantees a comparable level of protection of personal data to that in the EU.

FFOD with the US has been constrained over recent years, due to the lack of an adequacy agreement. In October 2022, the U.S. and the EU agreed on an EU-U.S. Data Privacy Framework[157]. It aims to ensure that European personal data is safe when transferred to U.S. soil. The agreement is now under revision. It

151 Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade,' International Data Privacy Law 10, no. 3 (August 2020): 201-22, https://doi.org/10.1093/idpl/ipaa003.

152 European Data Protection Supervisor, 'Data protection is non-negotiable in international trade agreements,' EDPS press release (February 2021), https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en. European horizontal provisions can be seen here: European Commission, 'EU proposal for provisions on Cross-border data flows and protection of personal data and privacy,' EU proposal (July 2018), http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf.

153 Kristina Irion, 'Chapter 11 - Panta Rhei: A European Perspective on Ensuring a High Level of Protection of Human Rights in a World in Which Everything Flows,' in 'Part III - Safeguarding Privacy and Other Users' Rights in the Age of Big Data' of *Big Data and Global Trade Law*, edited by Mira Burri (Cambridge University Press: July 2021): 231-242, https://www.cambridge.org/core/books/big-data-and-global-trade-law/panta-rhei/B0E5D7851240E0D2F4562B3C6DFF3011#.

154 'Convention 108 + Convention for the protection of individuals with regard to the processing of personal data,' Council of Europe (June 2018), https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

155 European Digital Rights, 'WTO trade talks must respect privacy: Together with over 40 consumer and digital rights groups, EDRi calls on global governments to place people's fundamental rights to data protection and privacy at the centre of digital trade negotiations,' *EDRi* (November 2020), https://edri.org/our-work/wto-trade-talks-must-respect-privacy/.

156 Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models,' *Nature Communications 10*, no. 1 (July 2019), https://www.nature.com/articles/s41467-019-10933-3.

157 European Commission, 'Questions & Answers: EU-U.S. Data Privacy Framework,' EU press corner Q&A (October 2022), https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

still may be challenged in the Court of Justice of the EU, given the lack of a national privacy law in the U.S. and the surveillance practices of U.S.-based Big Tech firms and government. A group of privacy organizations has asked that negotiations on a new transatlantic data transfer agreement should be paused until the U.S. Congress passes comprehensive privacy legislation and reforms U.S. surveillance laws.[158]

## 6- ... PROTECTION OF WORKERS IN THE EU?

### Skewing the Balance of Power between Corporations and Workers

One of the main features of hyperglobalisation is corporations using their outsized profits to rig the rules of the global economy - including through trade agreements. They have done this to redistribute income upward to themselves and their highly paid executives, and away from the people whose work produces the profits. Corporations have thus been able to capture an increasing percentage of the value of production from the labour of working people, driving down their collective power and entrenching a vicious cycle of loss of power and income share.

Writ large, the "digital trade" proposals in trade agreements represent an effort by Big Tech to further consolidate that upward distribution of income from labour to capital.

Corporations have captured the vast majority of productivity gains deriving from advances in technology and expanded technological use over the past several decades. Corporations have unduly controlled policy measures and have restructured industries to reduce workers' share of profits.[159] In discussions on the future of work, the emphasis on job retraining and skill-based technological growth can be useful but should not be a distraction. The most important aspect in shaping who will benefit from expanded technological use will be the policy environment in which that technology is utilized. Those policies are shaped at the local, sector or national level through collective bargaining, and/or at national level through laws, but also at the global level through trade treaties. If workers are not guaranteed their fundamental rights, freedom and autonomy in digitalised workplaces, and if workers do not have a governance stake in the data produced by workers, and instead this data is allowed to be "owned" by the collecting corporation, it will permanently skew the balance of power in further favour of corporations.[160]

Whether workers should have economic rights to the data they produce or help produce is a subject being debated. Locking data related commitments under trade agreement will make any such thing impossible, likely leading to a permanent suppression of labour's collective bargaining power in a digital age.

### Algorithmic Labour Abuses

Corporations are increasingly using algorithmic systems to manage workers. The use of automated hiring/firing systems, scheduling tools, worker productivity enhancing systems such as movement and location tracking systems to real-time surveillance and monitoring systems have resulted in a range of harms to workers. These range from discrimination, work intensification, mental and physical health abuses, to an erosion of fundamental labour rights such as the freedom of association and the right to collective bargaining. All of these harms can only be rectified if the algorithmic systems are subject to inclusive governance and the systems can be adjusted. If source code cannot be reviewed yet is faulty, there is no accountability and no remedy for the harms.

This is especially true in "platform work" which the EU is also currently looking to regulate better through the Platform Work Directive[161] against the vociferous lobbying of companies like Uber.[162] One of the main demands from trade unions with regards to platform work is algorithmic transparency.[163] As a resolution by the European Trade Union Confederation puts it: "free access to the source code must be ensured before the implementation of the AI system in the

158 Organized by the Transatlantic Consumer Dialogue (TACD) to President Joseph R. Biden (June 10, 2021), https://tacd.org/wp-content/uploads/2021/06/20210610-Data-Flows-Negotiations-Coalition-Letter-June2021.pdf.
159 UNCTAD, 'Corporate Rent-Seeking, Market Power and Inequality: Time for a Multilateral Trust Buster?' *UNCTAD* Policy Brief no. 66 (May 2018), https://unctad.org/en/publicationslibrary/presspb2018d3_en.pdf.
160 Parminder Jeet Singh, 'Economic Rights in a Data-Based Society: Collective Data Ownership, Workers' Rights, and the Role of the Public Sector,' *Friedrich Ebert Stiftung and Public Services International* (January 2020), https://library.fes.de/pdf-files/iez/16034.pdf.
161 Théo Bourgery-Gonse, 'EU institutions inch closer to an agreement on platform worker status,' Euractiv (September 2022), https://www.euractiv.com/section/economy-jobs/news/eu-institutions-inch-closer-to-an-agreement-on-platform-worker-status/.
162 Ludovic Voet, 'Uber's shadow looms over platform workers directive debates,' Euractiv (October 2022), https://www.euractiv.com/section/sharing-economy/opinion/ubers-shadow-looms-over-platform-workers-directive-debates/.
163 Aída Ponce Del Castillo and Diego Naranjo, 'Regulating algorithmic Management: An assessment of the EC's draft Directive on improving working conditions in platform work,' *European Trade Union Institute* Policy Brief (August 2022), https://etui.org/publications/regulating-algorithmic-management.

workplace."[164] International best practice, as highlighted in union negotiation guides,[165] is for a regular independent auditing of algorithms used for management. Yet, the EU-supported digital trade provision for a ban on source code would undermine this type of transparency.[166]

Algorithmic tools are increasingly utilized in white collar as well as blue collar and services industries, not just in "gig" workplaces. In a well-known example of algorithmic bias, Amazon developed an automated hiring system, but had to stop using it as it only hired men. As the algorithm learned from historical data, it learnt that there were more men than women working in technology. Masculinity was thus classified as something positive - and the system downgraded all applications with references to words such as woman or female.[167]

Trade union stewards, workers' legal defence teams, and workers themselves should have access to the data, and the algorithms, on which decisions regarding their employment are based. Unions should be able to collectively bargain on the use of technology, AI, and algorithmic decision-making, and access to code is key for this. The law should also recognise (and protect) this as an area of collective bargaining. All deployers of algorithmic systems should be legally obliged to conduct ongoing governance of (semi)automated systems, and this governance should include representatives of those who are subject to the systems: in this case the workers. Co-governance of these systems is a prerequisite to enforcing labour rights in this regard.[168] Labour regulators should have a priori consideration and approval of any algorithmic system and data sets that would be used in ways that affect workers' rights on the job. Certification and standards bodies must be balanced and include worker organizations on par with industry, and all certifications must be accompanied by the obligation of periodic and inclusive governance of the systems deployed.[169] Inspiration can here be found in the Spanish law that enables workers access to information on their characteristics and technical details,[170] as well as in the requirement in the GDPR that the Data Protection Impact Assessment (DPIA) should be periodically reviewed (i.e. governed). These remedies would be proscribed under the EU's digital trade proposals barring requirements to disclose source code and barring data localisation requirements.

## Reducing Potential for Job Creation

Big Tech's top goal is to force governments to allow them to collect, use, transfer, store, and share data as they please. The production of data is the central feature of the digital economy of the future, and most people are only just beginning to appreciate the value of data. The firms able to collect the biggest data sets will train their AI more accurately and will thus dominate their industries. Investors realize the value of data for future profits, and the corporations that are the largest data collectors enjoy the greatest market capitalization. Allowing Big Tech unfettered control over data would constrain policies to foment job creation, as countries need to harness the data sourced in their countries digital industrialization to create jobs, and to add value to existing jobs. The privatization of data that is central to the "digital trade rules" would severely limit states' ability to ensure widespread job creation and full employment through digitalization as well as a fair distribution of the income generated.

## Furthering Privatization

Digital trade proposals by the EU include demands to expand liberalization obligations on financial services, telecommunications, and computer services, especially to supply them across the border.[171] The reality that most production now depends on services, especially digital services, means these new obligations would also impact on workers in manufacturing, transportation, and even agricultural and food processing, as well as in retail, according to the global union federations in those sectors. The supply of those digitalized services from offshore undermines domestic jobs, pay and conditions.

164 European Trade Union Confederation, 'Resolution on the European strategies on artificial intelligence and data,' ETUC Executive Committee resolution (July 2020), https://www.etuc.org/en/document/resolution-european-strategies-artificial-intelligence-and-data.
165 See Patrick Briône, 'Algorithmic Management: A Trade Union Guide,' UNI Global Union's Professional & Managers group (September 2020), https://uniglobalunion.org/report/algorithmic-management-a-trade-union-guide/.
166 Anne Dufresne and Cédric Leterme, 'App Workers United: The struggle for rights in the gig economy,' *The Left in the European Parliament* (January 2021), https://left.eu/issues/publications/app-workers-united-the-struggle-for-rights-in-the-gig-economy/.
167 Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women,' *Reuters* (October 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
168 See Christina Colclough, 'Co-Governance of Algorithmic Systems – a guide,' *Why Not Lab* slide deck (November 2021), https://www.thewhynotlab.com/_files/ugd/aeaf23_62a52b0671c2466e999b2064c0cdb95b.pdf.
169 Colclough, 'Union Brief: G7 Digital Policy Priorities 2022,' Why Not Lab (2022).
170 Carlos del Castillo, 'Trabajo lanza una herramienta para facilitar la transparencia de los algoritmos laborales,' *El Diario* (June 2022), https://www.eldiario.es/tecnologia/trabajo-lanza-herramienta-facilitar-transparencia-algoritmos-laborales_1_9071089.html.
171 Jane Kelsey, 'Digital Trade Rules and Big Tech: Surrendering Public Good to Private Power,' Friedrich Ebert Stiftung and Public Services International (February 2020), https://pop-umbrella.s3.amazonaws.com/uploads/83f0b3b9-516e-49d7-8753-8c668d4f8c95_2020_-_ASIA_DIG_REPORT__1_.pdf.

Proposed rules would enable corporations to increase their outsourcing of service sector jobs. Trade provisions that guarantee corporations the right to transfer data across borders — free from requirements that they maintain a local presence in the country in which they are making profits, that they pay taxes, transfer technology, ensure privacy, or are held liable for any harm they cause — make it easier for them to relocate jobs around the world to wherever is most profitable. This often means outsourcing work to low-wage countries with rampant labour rights abuses.

Jobs affected include those in call centres, data processing, financial services, medical billing, logistics, and many more.[172]

## Labour Rights Abusing Corporations Seek New Limits on Big Tech Regulation

Corporate proponents of digital trade rules are some of the worst violators of labour rights. Many of the jobs they generate pay low and sometimes substandard wages,[173] violate international labour standards, and lack employment benefits. Amazon, accused of "exporting American working conditions to Europe,"[174] is being targeted by trade unions globally for its exploitative labour practices, including spying on workers' exercising their labour rights,[175] and the firing of workers organizing for better health protections during the COVID-19 crisis.[176]

Indeed, some Big Tech firms' business model is based on abusing precarious and informal labour, such as content moderators in Africa responsible for removing violent and illegal content on Facebook, who are paid as little as $1.50 USD per hour while suffering from mental illnesses including post-traumatic stress disorder (PTSD), anxiety, and depression.[177] Even more well-known is Uber's path of breaking EU labour laws and then deploying high-level lobbyists and weaponizing drivers to pressure officials to bend the laws to suit the company's profits, as revealed by a whistle-blower.[178] Such firms should not be granted further rights and protections in "trade" agreements, including from provisions that directly target their rights.[179]

More broadly, any global agreement on digitalization should focus on ensuring that digital and platform workers have quality, living wage union jobs. A primary source of digital firms' profits is the "disrupted" labour market in which one of their main "innovations" is making work more precarious. They are renowned for classifying platform workers as self-employed contractors, to evade their being covered by labour law (because they are independent contractors). Under this classification, however, if they unionise the workers can be considered a cartel, not a union. There has been progress on worker classification since the early Uber days, but most countries' legal frameworks are yet to be updated to ensure proper classification as workers.

Corporations increasingly take advantage of digitalization to locate jobs where workers have the weakest labour protections and the lowest wages. Many trade agreements include provisions that bar governments from requiring a local presence, which limits the ability of workers to collectively bargain and to hold them accountable for violating workers' rights. This has led to a race to the bottom in labour standards, thus putting downward pressure on wages and working conditions across Europe. Trade unions have called on governments to establish fair rules regarding competition, working conditions, and ensuring workers' rights for all workers, including "contract" workers. There is no path toward shared prosperity from digitalization and technological transformation that does not put universal employment and quality jobs with workers' freedom to organize at the centre of that transformation.

172 Kelsey, 'Digital Trade Rules and Big Tech,' FES and PSI (2020).
173 Julia Carrie Wong, 'Revealed: Google illegally underpaid thousands of workers across dozens of countries: Documents show company dragged feet to correct disparity after learning it was failing to comply with laws in UK, Europe and Asia,' *Guardian* (September 2021), https://www.theguardian.com/technology/2021/sep/10/google-underpaid-workers-illegal-pay-disparity-documents.
174 Albert Samaha, 'How Amazon Exported American Working Conditions To Europe: After Amazon workers in Germany began striking, the company expanded eastward, where looser labor laws brought record productivity,' *Buzzfeed News* (June 2022), https://www.buzzfeednews.com/article/albertsamaha/amazon-poland-slovakia-czechia-germany-labor-laws.
175 Lauren Kaori Gurley, 'Secret Amazon Reports Expose the Company's Surveillance of Labor and Environmental Groups: Dozens of leaked documents from Amazon's Global Security Operations Center reveal the company's reliance on Pinkerton operatives to spy on warehouse workers and the extensive monitoring of labor unions, environmental activists, and other social movements,' *Vice Motherboard* (November 2020), https://www.vice.com/en/article/5dp3yn/amazon-leaked-reports-expose-spying-warehouse-workers-labor-union-environmental-groups-social-movements.
176 UNI Global Union, 'Global Union Alliance: 'Amazon cannot fire its way out of this crisis,'' UNI Global Union (April 2020), https://uniglobalunion.org/news/global-union-alliance-amazon-cannot-fire-its-way-out-of-this-crisis/; Melissa Heikkilä, 'Amazon workers in France, Italy, Spain & Poland strike over labour conditions during COVID-19 pandemic,' Politico EU re-upped in Business & Human Rights Resource Centre (March 2020), https://www.business-humanrights.org/en/latest-news/amazon-workers-in-france-italy-spain-poland-strike-over-labour-conditions-during-covid-19-pandemic/.
177 Bill Perrigo, 'Inside Facebook's African Sweatshop,' *Time* (February 2022), https://time.com/6147458/facebook-africa-content-moderation-employee-treatment/.
178 Paul Lewis et al, 'The Uber whistleblower: I'm exposing a system that sold people a lie,' *Guardian* (July 2022), https://www.theguardian.com/news/2022/jul/11/uber-files-whistleblower-lobbyist-mark-macgann; see also, 'Explainer: What are the Uber files? A guide to cab-hailing firm's ruthless expansion tactics,' Guardian (July 2022), https://www.theguardian.com/news/2022/jul/10/what-are-the-uber-files-guide.
179 In just one example, while pitching its workplace app to clients, Facebook highlighted that employers could monitor workers' posts, such as whether someone used the word "unionize." Lee Fang, 'Facebook Pitched New Tool Allowing Employers to Suppress Words Like 'Unionize' in Workplace Chat Product,' *Intercept* (June 2020), https://theintercept.com/2020/06/11/facebook-workplace-unionize/.

### No Proposals Incorporate Demands from Trade Unions

The most important strategy to ensure digitalization's widespread and inclusive benefits is a commitment to full employment focused on equity, including strong labour rights and decent work and working conditions for all workers; gender and racial equity; and prohibitions on discrimination. This would include workers' rights in the digital context such as to their own data, and comprehensive and portable social protections (such as paid sick leave and unemployment insurance), including for workers now misclassified as contractors. It would include that public procurement contracts, including for digitalization of public services, go to businesses with collective bargaining rights. Yet none of the proposals made by labour unions and other pro-worker organizations are included in the digital trade rules under consideration.

For these reasons and more, in March 2020, the European Trade Union Confederation called on "the EU and its member states to freeze the plurilateral negotiations on e-commerce," further noting that they have "severe reservations about the WTO as the forum to negotiate data governance issues and shape the rules of the digital change, as the organization lacks expertise, mandate, does not involve trade unions adequately and has a reductive approach to rules-making."[180]

## 7- ... PROTECTION OF MINORITIES AGAINST DISCRIMINATION?

There is a growing body of evidence that AI can exacerbate discrimination and cause harm, either through faulty algorithms which "learn" patterns based on past inequities, or by exacerbating inequalities found in data sets used for training.[181] Depending on the sphere, the EU protects against discrimination based on characteristics including, but not limited to, nationality and place of residence, disability, religion or belief, racial and ethnic origin, and gender, sexual orientation, and age.

Algorithms are extensively utilized in search engines and advertising which result in harmful discrimination against women, people from immigrant communities, and people from other backgrounds that are regularly targeted.[182] Racial bias in algorithms has been documented in voter suppression, housing discrimination, predatory lending, insurance, employment discrimination,[183] and government surveillance and policing.[184] A few examples include search engine results that show job results based on the algorithmically-determined perceived race, ethnicity, or gender of the searcher,[185] and credit ratings or insurance premiums being decided based on ethnic or geographical origin, according to a report prepared for the European Commission.[186] The incredible failure rate of facial recognition technologies in distinguishing darker skinned people as compared to lighter skinned people, is well-documented and a serious cause for alarm.[187]

Algorithms used by surveillance advertising such as Facebook have been shown to magnify racist hate speech[188] as well as inaccurate, controversial, and inflammatory information, which has sometimes led to violent racist attacks, such as against immigrants in Germany[189] or against Black footballers in the UK[190] as two examples amid extensive scholarship on racism exacerbated by social media.[191]

This is not only an issue in the private sector, but also the public sector. The recent debacle in the childcare benefits system of the Netherlands exposed the extensive harm that the use of algorithms, unsupervised by human oversight, caused to the Dutch public.[192] In this massive scandal, use of algorithms to detect potential fraud in public welfare benefits led to over 1,000 children being put into

180 European Trade Union Confederation, 'ETUC position on the plurilateral negotiations on e-commerce," ETUC position adopted at Executive Committee Meeting (March 2020), https://www.etuc.org/en/document/etuc-position-plurilateral-negotiations-e-commerce.
181 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Polity: 2019).
182 Noble, *Algorithms of Oppression* (2018).
183 Ibid.
184 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press: 2018).
185 Alina Köchling and Marius Claus Wehner, 'Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development,' *Business Research 13* (November 2020): 795–848, https://doi.org/10.1007/s40685-020-00134-w.
186 Janneke Gerards and Raphaële Xenidis, 'Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law,' European Commission Directorate-General for Justice and Consumers (2020), https://www.equalitylaw.eu/downloads/5361-algorithmic-discrimination-in-europe-pdf-1-975.
187 See for example: Patrick Grother, Mei Ngan, and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,' *National Institute of Standards and Technology Report 8280* (December 2019), https://doi.org/10.6028/NIST.IR.8280.
188 Andrew Jakubowicz, 'Algorithms of hate: How the Internet facilitates the spread of racism and how public policy might help stem the impact,' *Journal & Proceedings of the Royal Society of New South Wales 151*, part 1 (2018): 69–81, https://search.informit.org/doi/10.3316/informit.790571095083969.
189 Amanda Taub and Max Fisher, 'Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests,' New York Times (August 2018), https://www.nytimes.com/2018/08/21/world/europe/facebook-refugee-attacks-germany.html
190 Luca Bertuzzi, 'Online racial abuses in the UK prompt calls to end anonymity online,' Euractiv (July 2021), https://www.euractiv.com/section/digital/news/online-racial-abuses-in-the-uk-prompt-calls-to-end-anonymity-online/.
191 Ariadna Matamoros-Fernández and Johan Farkas, 'Racism, Hate Speech, and Social Media: A Systematic Review and Critique,' *Television & New Media 22*, no. 2 (February 2021): 205-224, https://doi.org/10.1177/1527476420982230.
192 Melissa Heikkilä, 'Dutch scandal serves as a warning for Europe over risks of using algorithms,' *Politico EU* (March 2022), https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

foster care. Having proper public oversight over the use such AI could have caught the use of harmful data sets and poor algorithms.

In 2019, the EC published a White Paper on Artificial Intelligence, which recognised that the increasing use of algorithms in Europe poses specific risks in terms of fundamental rights and in particular in terms of equality and non-discrimination.[193] These risks are also recognised by the Commission's recent Gender Equality Strategy 2020-2025, which acknowledges that AI "risks intensifying gender inequalities."[194]

In the lead-up to the drafting of the DSA and AI Act, several studies identified algorithmic racial or ethnic, gender[195], and LGBTQIA+[196] discrimination as problematic. A coalition of civil society organizations led by EDRi, including Algorithm Watch, the European Disability Forum, the European Network Against Racism, UNI Europa, and others, called for red lines in the AI Act for threats to fundamental freedoms.[197] These included clear limitations on the use of AI in migration control; the use of AI in social scoring and determining access to social rights and benefits; predictive policing which repeatedly score poor, working class, racialised and migrant communities with a higher likelihood of presumed future criminality; and the use of risk assessment tools in the criminal justice system and pre-trial context; all of which threaten fundamental rights particularly among racialized communities.

Further, recent studies have shown that source codes and algorithms which are inter-connected and learn from themselves (machine-learning)[198] can lead to many undesired outcomes which include discrimination based on income, colour and gender. Recognizing this, the UN Committee on the Elimination of Racial Discrimination has stressed that algorithmic profiling systems should be in full compliance with international human rights law.[199] It has underscored the importance of transparency in the design and application of algorithmic profiling systems when they are deployed for law enforcement purposes. In its recommendations the Committee emphasizes, "[t]his includes public disclosure of the use of such systems and explanations of how the systems work, what data sets are being used and what measures preventing human rights harms are in place."[200]

But digital trade proposals proscribe states from requiring source code disclosure. They do contain exceptions to allow disclosure of source codes and algorithms to requesting judicial or regulatory authorities for investigations, and the EU-NZ FTA uniquely expands this to include discrimination and bias. But the Conference of the Federal and State Ministers for Equality of Germany "pointed out that, due to the complexity of the matter, it seemed unrealistic that those affected would be able to detect and pursue algorithmic discrimination."[201] As noted previously, transparency remedies must also be available for affected parties, researchers, critical engineers, advocates, trade union stewards, and the general public – not just for governments.

If algorithmic systems might violate fundamental and human rights to be free of discrimination, AI systems should have to be proven not to do so in advance of their deployment – not after harms are suffered. And policies upholding human and fundamental rights should not be subject to adjudication in trade tribunals, which prioritize trade issues over the rights of affected communities.

## 8- ... THE EU'S GREEN DEAL AGENDA?

The European Green Deal sets out a roadmap of how to make Europe the first climate-neutral continent by 2050 while boosting the economy, improving people's health and quality of life, and leaving no one behind, according to the European Commission.[202]

193 European Commission, 'White Paper on Artificial Intelligence: A European approach to excellence and trust,' European Commission COM(2020) 65 final (February 2020): 3 and 11, https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
194 European Commission, 'Communication: A Union of Equality: Gender Equality Strategy 2020-2025,' European Commission COM(2020) 152 final (March 2020): 'Challenging gender stereotypes' section, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0152.
195 Fabian Lütz, 'Gender equality and artificial intelligence in Europe. Addressing direct and indirect impacts of algorithms on gender-based discrimination,' *ERA Forum 23* (April 2022): 33-52, https://doi.org/10.1007/s12027-022-00709-6.
196 Christina Dinar, 'The state of content moderation for the LGBTIQA+ community and the role of the EU Digital Services Act,' *Heinrich-Böll-Stiftung* (June 2021), https://eu.boell.org/en/platform-moderation-lgbtiqa-DSA.
197 Letter organized by European Digital Rights to European Commission, 'Open letter: Civil society call for the introduction of red lines in the upcoming European Commission proposal on Artificial Intelligence' (January 2021), https://edri.org/our-work/civil-society-call-for-ai-red-lines-in-the-european-unions-artificial-intelligence-proposal/.
198 Harold Feld, 'The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms,' *Roosevelt Institute* (May 2019), https://rooseveltinstitute.org/wp-content/uploads/2020/07/RI-Case-for-the-Digital-Platform-Act-201905.pdf.
199 UN Human Rights Committee on the Elimination of Racial Discrimination, 'UN Committee issues recommendations to combat racial profiling,' UN General Comments and Recommendations (November 2020), https://www.ohchr.org/en/general-comments-and-recommendations/2020/11/un-committee-issues-recommendations-combat-racial.
200 Ibid.
201 See footnote 366 cited in Gerards and Xenidis, 'Algorithmic discrimination in Europe,' European Commission (2020): 87.
202 European Commission, 'A European Green Deal,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.

The EU's Trade Policy states that it "should unequivocally support the Green Deal in all its dimensions, including the ambition to achieve climate neutrality by 2050."[203]

The Green Deal promotes new technological innovation to resolve the world's climate crisis. But for the entire world to make the necessary transitions, transfers of climate-reducing technology innovations to ensure their global use will be required. Bans on source code disclosure, and other forms of technology transfer, will render the achievement of the Paris Agreement impossible.

Countries also need tax revenue (for example, from taxing Big Tech) in order to fund their transition. Big Tech's proposals to limit the ability of states to tax their operations and cross-border delivery of electronic goods and services will reduce those needed investments.

Global e-commerce in goods further displaces local production in favour of international goods, but these can be more climate intensive due to transnational shipping costs.[204]

The hyper-concentrated and data hungry digital economy promoted by Big Tech and the proposed digital trade rules is also radically at odds with the fight against global warming. The carbon footprints of training AI or operating a hyperscale data centre are far beyond the required limits set by the Paris Agreement. The footprint of the world's tech industries is three times that of France, in terms of energy, materials, and water consumption, according to a Paris-based think tank. The digital economy uses 10 percent of the world's electricity and generates nearly 4 percent of global CO2 emissions, almost twice as much as the civil aviation sector.[205]

The over-utilization of domestic energy supplies is becoming such an issue that countries such as Ireland, holding 25 percent of the European data centre market, are facing calls for a moratorium on the construction of new data centres.[206] At a time when European consumers are being called on to cut down on energy usage due to the war in Ukraine, data centres are being increasingly scrutinized by regulators and the public.[207] A European Commission study predicts that data centres will use 18.5 percent more energy from 2018 to 2030.[208]

The same is true for water consumption. Local activists in Zeewolde (near Amsterdam) forced Meta to abandon plans to build an energy-intensive data centre there in July 2022,[209] after revelations that Microsoft's giant data centre complex in North Holland consumed 84 million litres of water during 2021, a year when heat caused severe water shortages.[210] Data centres require high volumes of water directly for cooling purposes and indirectly, through electricity generation.[211] Some data centres are located in water-stressed regions prone to droughts and water shortages. These sometimes result in conflict with local communities, or restrictions on water usage. Environmental, social and governance researchers are even taking these risks into consideration in assessing business risk.[212]

203 European Commission Directorate-General for Trade, 'Communication: Trade Policy Review,' European Commission COM/2021/66 final (2021).
204 Theresa Kofler et al, 'Policy Brief on Digital Trade,' *Seattle to Brussels network* (April 2022), http://s2bnetwork.org/wp-content/uploads/2022/04/S2B-DigitalTrade-policybrief.pdf.
205 Hugues Ferreboeuf and working group, 'Lean ICT: Towards Digital Sobriety,' *Shift Project* (March 2019), https://theshiftproject.org/en/article/lean-ict-our-new-report/.
206 Pádraig Hoare, 'Energy use of data centres equivalent to powering 200,000 homes,' *Irish Examiner* (May 2022), https://www.irishexaminer.com/news/arid-40864262.html.
207 April Roach and Ewa Krukowska, 'Big Tech Gets Caught Up in Europe's Energy Politics: As the war in Ukraine threatens supplies, some countries are pushing for tighter control over data centers that consume vast amounts of electricity,' Bloomberg (June 2022), https://www.bloomberg.com/news/articles/2022-06-23/google-facebook-data-centers-face-europe-political-snags-over-in-energy-crisis.
208 European Commission Directorate-General for Energy, 'Green and Digital: study shows technical and policy options to limit surge in energy consumption for cloud and data centres,' European Commission news article (November 2020), https://ec.europa.eu/info/news/green-and-digital-study-shows-technical-and-policy-options-limit-surge-energy-consumption-cloud-and-data-centres-2020-nov-09_en.
209 Georgia Butler, 'Meta data center in Zeewolde facing opposition by Dutch Housing Minister: Former Deputy PM Hugo de Jonge hopes stricter requirements for data centers will prevent the development of the hyperscale,' DatacenterDynamics (March 2022), https://www.datacenterdynamics.com/en/news/meta-data-center-in-zeewolde-facing-opposition-by-dutch-housing-minister/.
210 Peter Judge, 'Drought-stricken Holland discovers Microsoft data center slurped 84m liters of drinking water last year – After the company and local authority said the facility would only need 12 to 20 million liters,' DatacenterDynamics (August 2022), https://www.datacenterdynamics.com/en/news/drought-stricken-holland-discovers-microsoft-data-center-slurped-84m-liters-of-drinking-water-last-year/.
211 David Mytton, 'Data centre water consumption,' *npj Clean Water 4* (February 2021), https://doi.org/10.1038/s41545-021-00101-w.
212 Erin Johnson and Kata Molnar, 'ESG Risks Affecting Data Centers: Why Water Resource Use Matters to Investors,' Sustainalytics (August 2022), https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/esg-risks-affecting-data-centers-why-water-resource-use-matters-to-investors.

A recent proposal by the Climate Neutral Data Centre Pact to pre-empt upcoming legislative mandates to reduce water use to a maximum of 400ml per kWh of computer power by 2040[213] could help address this; but without limiting the total computer power, the net impact is yet to be seen, particularly given that the group has come under fire for becoming a vehicle for U.S.-based Big Tech lobbying rather than achieving green goals.[214] Instead, the Commission's plan calling out data centres' environmental impact[215] should include binding targets.

Beyond energy and water consumption, the Sustainable Digital Infrastructure Alliance has identified priorities towards a sustainable digital economy including by emissions, electronic waste, other resource consumption, pollution, and socioeconomic issues, all of which are a concern given the burgeoning and uncontrolled pace of digital infrastructure.[216]

Sustainable digitalization cannot co-exist with huge digital monopolies pushing for ever more collection, storing and processing of data on a global scale.

## 9- ... THE EU'S REGULATION OF BIG TECH MONOPOLIES?

European regulators and legislators have become well aware of the negative impacts of Big Tech's monopoly practices and powers. Europe has engaged in the most extensive enforcement actions against Big Tech. Reducing Big Tech's market dominance and regulating their practices to set a level playing field to ensure fair competition will have clear benefits for all aspects of European society, and especially for digital industrialization and SMEs, as discussed in other sections.

But Big Tech is working feverishly to undermine and constrain efforts to reduce market dominance and anti-competitive practices in the tech sector through certain provisions in digital trade agreements. These include expanding existing "market access" rules through the "Understanding on Computer and Related Services," bans on source code disclosure requirements, interoperability provisions, and bans on local presence requirements.

### Expanding Market Access through the Understanding on Computer and Related Services (UCRS)

One of the EU's primary goals in the digital trade negotiations is to expand the services which are subject to these "market access" rules by having other members agree to its proposed "Understanding on Computer Related Services (UCRS)."

These market access rules greatly constrain "measures" that "affect" the supply of services, including competition policies in restricting size, market share, or restrictions on digital services and suppliers. The UCRS would "guarantee digital infrastructure firms have virtually unrestricted access into countries and rights to operate there with very limited regulation."[217]

The UCRS aims to make all computer-related services automatically subject to these rules, even if they were not invented at the time that countries took the original commitments.[218] Countries that agree to the EU's UCRS agree to include market access commitments for "computer systems, programming including source codes and algorithms, maintaining computer systems and software, and processing and storage of data." The Understanding ensures that those commitments apply to all computer and related services, including online search engines, social media, digital marketplaces, online advertising or digital entertainment.

But it would also include those yet to be invented. According to a legal analysis, "that future-proofs the scope of computer and related services to include whatever new services and technologies might be developed in the future, but with no criteria for determining what additional elements might fall within its scope."[219]

Applying open-ended disciplines which restrict competition policy remedies to all digital services would benefit the monopolistic practices of Big Tech to the detriment of fair competition policies far into the future.

213 Peter Judge, 'European operators plan to cut water use to 400ml per kWh by 2040,' DatacenterDynamics (July 2022), https://www.datacenterdynamics.com/en/news/european-operators-plan-to-cut-water-use-to-400ml-per-kwh-by-2040/.
214 Mathieu Pollet, 'Alliance for green data centres shows cracks over water consumption target,' Euractiv (June 2022), https://www.euractiv.com/section/digital/news/alliance-for-green-data-centres-shows-cracks-over-water-consumption-target/.
215 Pieter Haeck and Antonia Zimmermann, 'Europe's hidden energy crisis: Data centers: Brussels zones in on digital economy's heavy energy and water use,' Politico EU (October 2022), https://www.politico.eu/article/data-center-energy-water-intensive-tech/.
216 See Sustainable Digital Infrastructure Alliance's website here: https://sdialliance.org/.
217 Jane Kelsey, 'Understanding the European Union's Understanding on Computer and Related Services,' Third World Network (September 2019), https://www.twn.my/title2/briefing_papers/No101.pdf. Full investigation at https://www.twn.my/title2/FTAs/Services/Full%20report%20for%20TD%20series_FORMAT_Ver6-FIN-09012020.pdf.
218 Ibid.
219 Ibid.

### Bans on Source Code Transparency

As detailed below, the AI Act will require further investigation of algorithms classified as "high risk."

But many monopolistic practices occur in settings that may not meet this classification. For example, digital advertising may not be considered "high risk," but this sector is highly based on oligopolistic practices by Big Tech behemoths. Likewise, anti-competitive practices using algorithms are ubiquitous in the online retail sector, where companies like Amazon ensure that their search algorithms privilege their own products or services above those of others. There may be difficulty to bring a legal challenge because of lack of capacity to identify the source of the issue, or the standard of proof may be difficult to meet without access, or the agency may not have the expertise without being able to go outside but may be constrained in doing so by a requirement for "safeguards against unauthorised disclosure".

The new exceptions aim to make such investigations easier. But those rules still require a suspicion, as they relate to specific cases, and cannot require disclosure as a general rule, which creates a chicken and egg problem – individuals must know that they are being harmed and have a suspicion that it is because of the algorithm and convince the regulatory agency; or the regulatory body itself must be able to establish a prime facie basis to justify accessing the source code. In earlier agreements, exceptions related only to requirements to remedy, which assumes that parties can make their case and identify the problem and solution without access to the code (or in some agreements algorithms, although the relationship between them is sometimes unclear).

### Interoperability Rules

Big Tech often exclude other companies' products from their platforms or operating systems, in order to maintain monopoly control. For example, Apple excludes other digital payments systems from its app store. The EU recently mandated interoperability in the DSA. But Big Tech would like to maintain this monopolistic practice as a right. The most recent leaked version of the Joint Statement Initiative on e-commerce being negotiated at the WTO includes the provision: "No party/member shall prevent public telecommunications networks or their services suppliers, including value-added services, from choosing the supporting technologies of their networks and services, and/or electronic commerce-related network equipment and products related to the technologies."[220] This provision is written in a way as to preclude states from being able to require interoperability such as in app stores. While it is not included in EU digital trade agreements, its presence in the plurilateral the EU is negotiating at the WTO should raise concerns.

### Rules Banning Requirements that Firms Establish a Local Presence

For economies of scale, and for regulatory and tax arbitrage, Big Tech companies will choose which jurisdictions they operate out from. When they are cross border (Mode 1 in GATS jargon) it is extremely difficult to bring them within a domestic jurisdiction. The "no local presence" rule included in recent services chapters, which is part of Big Tech's wish list, facilitates this. So does the market access rule that says that states cannot require an entity that has a local presence to take a particular legal form, so it may not be legally responsible for the actions of the company it services. Serving legal papers on an entity in another jurisdiction is deeply problematic if it refuses to accept local service. That may require a time consuming, complex and expensive diplomatic process. Once served, getting the entity to submit to the jurisdiction is another battle. Then if both those are overcome, enforcement of the outcome also becomes problematic.[221]

The EU's leadership in finally bringing Big Tech behemoths to account for their anti-competitive behaviour, and its leadership in setting new rules to constrain monopolistic behaviour online, should not be undermined by stealth efforts by Big Tech to rig the rules in their favour.

## 10- ... EU SMES?

In 2021, 99.8 percent of all enterprises in the EU-27 non-financial business sector (NFBS) were SMEs. They employed 83 million people, the equivalent of 64 percent of total employment in the NFBS, and generated 52 percent of the total value added produced by the non-financial business sector.[222] The vast majority of EU-based SMEs that sell online use Big Tech online platforms to reach consumers. The market power differentials between SMEs and Big Tech are unprecedented in recent history.

220 E(2)(1)5 from September 2021 WTO draft.
221 I am grateful to Jane Kelsey for this important observation.
222 Patrice Muller et al, 'Annual Report on European SMEs 2021/22: SMEs and environmental sustainability,' European Commission (April 2022), https://single-market-economy.ec.europa.eu/smes/sme-strategy/sme-performance-review_en#paragraph_885.

SMEs are dependent on platforms' algorithms in terms of how their products are ranked in search results or are otherwise advertised. Businesses using Big Tech platforms do not have access to the data on their own customers and resulting from their own activity on the gatekeeper's platform, making it impossible for them to compete in a fair market – while the Big Tech platform can use such data for its own business purposes.

Digital trade provisions that bar states from being able to require algorithmic transparency or that copies of data be stored locally (in the case that the local business is domiciled in a different country than that of the gatekeeper platform) constrain remedies for these problems.

But these are just a few of the ways that Big Tech behemoths intend to use digital trade rules to establish global dominance. The entire suite of digital trade provisions was produced by Big Tech for their benefit. Rather than award the largest corporations new rights in binding, permanent treaties, rulemaking through these "trade" provisions should be put on pause until new rules that would benefit SMEs and reduce the power of Big Tech, including to vacuum up data globally, can be implemented.

In addition, European proposals include expanded commitments on "Computer and Related Services" described above which would "guarantee digital infrastructure firms have virtually unrestricted access into countries and rights to operate there with very limited regulation."[223] While some may see an opportunity to gain access to foreign markets for European firms, the first-mover and scale advantages of U.S.-based Big Tech would likely indicate that this dominance would be consolidated under such an approach.

Under a fully liberalized market access scheme for computer and related services, written as broadly as the EU proposal, it is difficult to see any scope for protecting or supporting European SMEs. Based on more recent and emerging concerns about the loss of market-share of European SMEs, the constraints on digital industrial policy space, and the call for European policy to support the diffusion of benefits to all Europeans from digitalization in the region, the digital trade rules, as supported by the EU since 2016, are outdated and not fit for today's world.

223 Kelsey, 'Understanding EU Understanding on Computer and Related,' TWN (2019).

# 6.

# WHO WILL BENEFIT FROM THE EU'S DIGITAL TRADE AGENDA?

One might wonder why European trade policy seems so oriented towards benefiting the largest big tech transnational corporations when nearly all of those are actually U.S.-based (or Chinese) and not European companies.

First of all, the "European" business lobbies are heavily dominated by U.S.-based Big Tech. Principal Europe-based trade groups lobbying for digital trade in the EU include DigitalEurope, Ecommerce Europe, and the European Services Forum. For example, DigitalEurope intervened repeatedly in the process of European digital legislation, including the deployment of Nick Clegg, former Deputy Prime Minister of the UK, in its top global lobby job.[224] But it represents the interests Amazon, Apple, Meta (Facebook) and Google, along with some European firms. Ecommerce Europe includes Amazon, eBay, and Etsy. The European Services Forum counts Apple, Google, IBM, Microsoft, Oracle, and UPS as members. Even BusinessEurope's Corporate Advisory and Support Group includes Apple, Meta, Google, Microsoft, Uber, Intel, IBM and Oracle.[225]

Second, along with "European" trade associations, the U.S.-based Big Tech trade associations also lobby heavily on digital trade. This includes the Computer & Communications Industry Association, the now-defunct Internet Association, the Information Technology Industry Council, the U.S. Council for International Business, the Coalition of Services Industries, and the National Foreign Trade Council.[226]

Third is the massive expansion of direct lobbying of EU officials by U.S.-based Big Tech. In a stunning report, "The Lobby Network: Big Tech's Web of Influence in the EU,"[227] Corporate Europe Observatory (CEO) and Lobbycontrol offer an overview of the tech industry's EU lobbying firepower. For the first time, they map the "universe" of actors lobbying the EU's digital economy, and they found a wide yet deeply imbalanced "universe":

- with 612 companies, groups and business associations lobbying the EU spend over €97 million annually lobbying the EU institutions. This makes tech the biggest lobby sector in the EU by spending, ahead of pharma, fossil fuels, finance, and chemicals.

- in spite of the varied number of players, this universe is dominated by a handful of firms. Just ten companies are responsible for almost a third of the total tech lobby spend: Vodafone, Qualcomm, Intel, IBM, Amazon, Huawei, Apple, Microsoft, Facebook and Google spend more than €32 million making their voices heard in the EU.[228]

The figures below represent the numbers from the research as they were self-reported in 2021; Google and Facebook, among others, have significantly increased their spending.

224 Nick Clegg, 'The next two years will define the next 20 for Europe's internet economy,' Medium (May 2021), https://nickclegg.medium.com/the-next-two-years-will-define-the-next-20-for-europes-internet-economy-8e02da6754da.
225 See companies listed on BusinessEurope's Corporate Advisory and Support Group website here: https://www.businesseurope.eu/about-us/asgroup-our-partner-companies.
226 Daniel Rangel et al, "Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies,' Rethink Trade (November 2022), https://rethinktrade.org/fact-sheet/digital-trade-doublespeak-big-techs-hijack-of-trade-lingo-to-attack-anti-monopoly-and-competition-policies/.
227 Max Bank et al, 'The Lobby Network: Big Tech's Web of Influence in the EU,' *Corporate Europe Observatory (CEO)* and *Lobbycontrol* (August 2021), https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf.
228 Bank et al, 'The Lobby Network,' CEO and LobbyControl (2021).

## TOP 10 LOBBY SPENDERS OF THE DIGITAL INDUSTRY

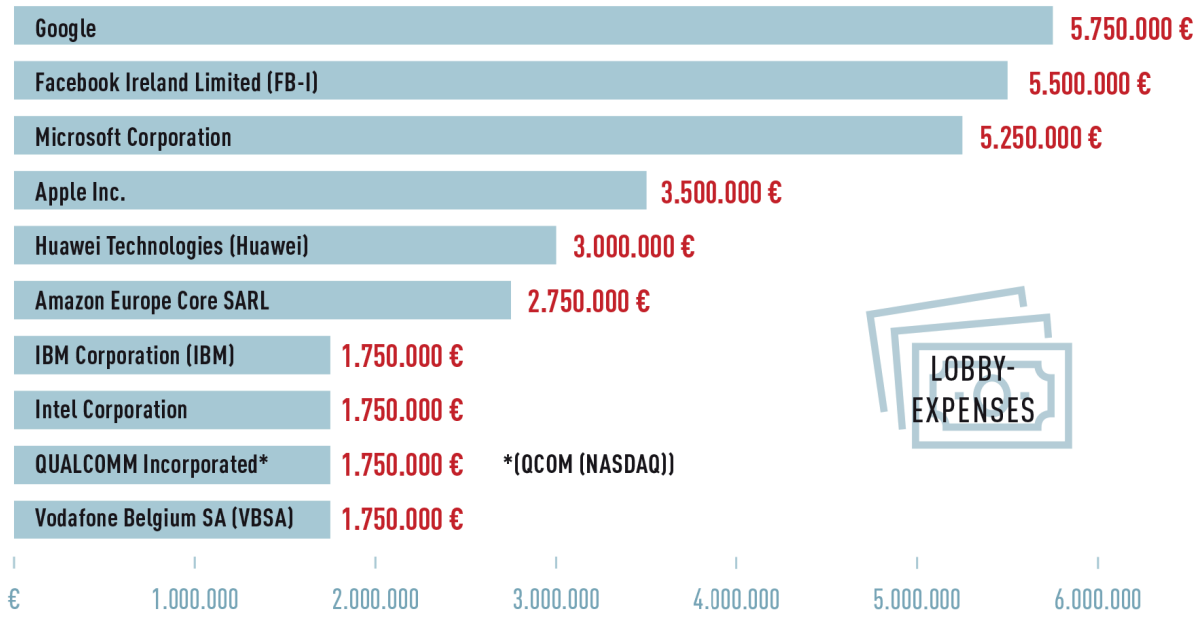



*Chart:* Corporate Europe Observatory & Lobbycontrol *Source:* EU Transparency Register

These tech corporations all expanded their lobbying budgets and staffing heavily in the last few years. "I have never seen something like that, at least not on this scale," said Bernd Meyring, a competition lawyer at Linklaters was quoted as saying in Politico. "Comparing this to any other industry is quite remarkable and that shows what's at stake for these companies."[229] They held myriad lobbying meetings with the Commission and MEPs, according to CEO, since the initial frameworks for legislative proposals were underway.[230]

Other leaks have corroborated this ramp-up, particularly emphasizing the specific lobbying exercised by Big Tech on the EU with regards to the WTO and free data flow.[231] A minor scandal even emerged after the leak of Google's lobby strategy – which included provisions such as "create 'pushback' against Commissioner Breton" and "create conflict between Commission departments."[232]

U.S. regulators have been reluctant to criticize the new European legislative initiatives,[233] perhaps given that they are debating these same issues domestically both in the U.S. Congress as well as federal agencies. But the EU-U.S. Trade and Technology Council is a classic example where "regulatory cooperation" is being used to stall or weaken legislation and is an entry point for industry lobbying, according to another report by CEO.[234]

229 Pietro Lombardi, 'Big Tech gears up for tougher regulatory environment in Europe,' *PoliticoPro* (March 2022), https://pro.politico.eu/news/147856.
230 'Big Tech brings out the big guns in fight for future of EU tech regulation,' *Corporate Europe Observatory* (December 2020), https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation.
231 Alexander Fanta, 'Tech industry pushes Europe for WTO data flows deal: Documents reveal the lobbying push by Microsoft, Google and other tech giants to influence secretive trade talks that could change the future of the internet,' Netzpolitik.org (June 2021), https://netzpolitik.org/2021/digital-trade-tech-industry-pushes-europe-for-wto-data-flows-deal/.
232 Emmanuel Berretta and Guillaume Grallet, 'Comment Google veut faire plier Bruxelles,' *Le Point* (October 2020), https://www.lepoint.fr/high-tech-internet/exclusif-comment-google-veut-faire-plier-bruxelles-28-10-2020-2398468_47.php.
233 Leah Nylen and Samuel Stolton, 'U.S. slow to respond to EU's landmark tech regulation,' *Politico* (March 2022), https://www.politico.com/news/2022/03/25/us-eu-digital-markets-act-00020551.
234 'Tech lobby eyes opportunities created by new EU-US Trade and Tech Council,' *Corporate Europe Observatory* (September 2021), https://corporateeurope.org/en/2021/09/tech-lobby-eyes-opportunities-created-new-eu-us-trade-and-tech-council.

These Big Tech behemoths are not content with direct lobbying influence, however. They have taken advantage of groups like the Climate Neutral Data Centre Pact to also wield power. European members of the pact have complained that "large U.S. data firms are instead using the pact as a lobbying vehicle. 'It's never really said, but their objective is to unite the actors of the industry and to be able to speak on its behalf,'"[235] said the manager of one of several European members quoted by Politico, speaking on the condition of anonymity. Signatories include Amazon Web Services, Google, and Microsoft.[236]

In October 2022, leading MEPs have asked for an investigation into Google, Meta (Facebook) and Amazon, as well as the Computer & Communications Industry Association and other trade lobby groups, calling for the firms to be banned from engaging with EU institutions.

The complaint states that the Big Tech companies deceived EU lawmakers in their lobbying efforts on the DSA and DMA by "pretend[ing]to be the official representatives of SMEs while at the same time promoting and defending the business interests of Big Tech," – but without disclosing their connections.[237]

Given this evidence, it is easy to see why EU trade policies are still being written to benefit Big Tech. And one could surmise that this is also happening with regards to trade policies in Japan, in Australia, in Canada, etcetera. Thus, arguments that "the entire developed world" favours such-and-so policy fall flat when one sees that the policies are emanating from the lobby efforts of the same few Big Tech corporations, based in the U.S.

235 Louise Guillot, 'How US tech is using a data center pact to lobby Brussels,' *PoliticoPro* (May 2022), https://www.politico.eu/article/us-tech-climate-neutral-data-center-pact-eu-lobbying-carbon-footprint-environment/.
236 See full list of signatories here: https://www.climateneutraldatacentre.net/signatories/.
237 Clothilde Goujard, 'Big Tech accused of shady lobbying in EU Parliament: Lawmakers file complaints against 8 companies and trade groups over alleged shadow lobbying,' *Politico EU* (October 2022), https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban/.

# 7.

# THE DIGITAL TRADE AGENDA VS. THE CURRENT EUROPEAN LEGISLATIVE AGENDA

The most recent overall EU trade policy, "An Open, Sustainable and Assertive Trade Policy," notes that the "EU should continue to lead the way in digital standards and regulatory approaches, in particular as regards data protection, where the EU's GDPR is often seen as a source of inspiration. To achieve this, the WTO needs to set the rules for digital trade and the EU needs to play a central role in creating them."[238]

However, the following analysis of the current legislative projects of the EU demonstrate that the EU trade policy is actually fundamentally in contradiction to the stated goals as well as the specific provisions of those initiatives and, if not substantially changed, could severely hamper the ability of the EU to enforce them.

The European Parliament and European Commission have approved, or are considering, a multiplicity of major legislative projects aimed at regulating the digital economy, in addition to the well-known GDPR, that could interplay with digital trade rules.[239] In addition to specific projects mentioned above, the most relevant and cross-cutting will be more thoroughly considered here.

Before reviewing specific laws, it should be noted that these are some of the first major steps for the EU in regulating the evolving digital economy, but they are not expected to be the last. As technologies accelerate, Big Tech invents new business models, and new threats emerge, legislators will need to maintain the policy space to address ongoing and new challenges. They should not be hamstrung in their cross-cutting legislative mandates by permanent "trade" constraints on their policymaking in this fast-changing field of the digital economy.

The EU's DSA and the DMA were introduced in December 2020, debated in several committees, and received extensive public input. They were subjected to heavy lobbying by the Big Tech industry that worked to weaken its public interest protections. They were approved in the European Parliament in July 2022, the Council shortly thereafter, and entered into force on November 1, 2022 (DMA)[240] and November 16, 2022 (DSA).[241]

They are both primarily concerned with online internet intermediaries and platforms such as online marketplaces, social networks, and app stores, with the stated goals of ensuring that the fundamental rights of all users of digital services are protected, and to establish a level playing field to foster innovation, growth, and competitiveness.[242] Many actors will be involved in implementation, with the Directorate-General for Communications Networks, Content and Technology (DG CNECT) and DG for Competition playing leading roles.

In addition, the DGA entered into force on 23 June 2022. Similarly, the AI Act and the DA were proposed by the European Commission in April 2021 and February 2022 respectively and are still undergoing the legislative progress.

**The above evidence of the negative impacts on European society of the provisions of the digital trade agenda begs the question of whether the**

238 European Commission Directorate-General for Trade, 'Communication: Trade Policy Review,' European Commission COM/2021/66 final (2021).
239 Cristiano Codagnone, Giovanni Liva and Teresa Rodriguez de las Heras Ballell, 'Identification and assessment of existing and draft legislation in the digital field: Study Requested by the AIDA Special Committee,' European Parliament study PE 703.345 (January 2022), https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)703345.
240 European Parliament, 'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance),' EU regulation PE/17/2022/REV/1 published at EUR-Lex (September 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC.
241 European Parliament, 'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance),' EU regulation PE/30/2022/REV/1 published at EUR-Lex (October 2022), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2065.
242 European Commission, 'The Digital Services Act package,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

**provisions on data flows, data localisation and non-disclosure of source codes are compatible with the new laws. The answer is clear that they are not at all compatible with the laws. They are even less compatible with the stated intentions of EU legislators, regulators, and leaders.**

## DSA[243]

The DSA introduces new obligations on online intermediaries and especially very large online platforms (VLOPs) and very large online search engines (VLOSEs)[244] that reach 10 percent of the EU population, or 45 million users, monthly. It bars targeted ads towards children as well as ads based on sensitive information (such as race or ethnicity, political views, sexual orientation, or religion). It requires firms to assess and mitigate systemic risks that arise from the "design, including algorithmic systems, functioning and use made of their services." The risk assessments must address issues such as illegal content; negative effects on many fundamental rights, civic discourse, electoral processes, and public security; and physical and mental health including the protection of minors and gender-based violence. These assessments would need to include algorithms such as advertising and recommender systems as well as data practices. VLOPs and VLOSEs will need to take reasonable, proportionate, and effective mitigation.

"This means that tech giants will have to become more accountable for the use of toxic content-shaping algorithms that are amplifying hate speech, disinformation or gender-based harassment, and that they will have to adapt the functioning and design of these recommender systems to avoid the spread of such harmful content," according to Amnesty International.[245]

Algorithmic transparency is key to the DSA. Regulators will need to set up a "European Centre for Algorithmic Transparency" to attract data and algorithm scientists to help with enforcement, although the funds proposed thus far have been criticized as insufficient. But comprehensive regulatory oversight over algorithms does not seem feasible, and will certainly be made more difficult, under the provision in the digital trade agreements which bar governments from being able to require the disclosure of the source code or algorithm except in very limited circumstances. As mentioned earlier, there are exceptions for prevention or remedies to competition restrictions or distortions, and public safety in Article 207 of the EU-UK TCA,[246] but only for specific investigations and ex post. The EU-NZ FTA also adds an exception for bias and removes the "specific" limitation.

However, exceptions for many other aims of the DSA, such as illegal content, fundamental rights, electoral manipulation, and others, do not appear in the provisions. Those who may rebut this claim by relying on the general exceptions imported into digital trade agreements from Article XX of the WTO's GATT should note that those exceptions do not directly relate to most of those policy objectives, can only be used as a defence in a case, and only two of 48 attempts to use these exceptions have ever succeeded in the WTO.[247]

Civil society organizations have called for the DSA to be strengthened with regards to ensuring transparency of algorithms and preventing Big Tech from using algorithms in ways that exacerbate the spread of disinformation, discrimination, manipulation, and undermine competition,[248] and for phasing out all intrusive surveillance-based advertising.[249]

After an inquest into the 2017 death of a 14-year-old girl, Molly Russell, the coroner concluded that social media had contributed, stating that she had "died from an act of self-harm whilst suffering from depression and the negative effects of online content".[250] The teen's father has urged legislators to put children's health and safety first and regulate content delivery.

243 'European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)),' European Parliament adopted text P9_TA(2022)0269 for vote PV 05/07/2022 - 6.4 for debate CRE 19/01/2022 - 14 on topic A9-0356/2021 (July 2022), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html#title2.

244 Defined as reaching an average of 45 million active users monthly, and predicted to include Alphabet's Google Search and YouTube, Amazon, Meta's Facebook and Instagram, TikTok, and perhaps Twitter.

245 'What the EU's Digital Services Act means for human rights and harmful Big Tech business models,' *Amnesty International* index: POL 30/5830/2022 (July 2022), https://www.amnesty.org/en/documents/pol30/5830/2022/en/.

246 Title III, Chapter 3, Article 207: Source Code, in the EU-UK TCA.

247 Rangel, 'WTO General Exceptions,' Public Citizen (2022).

248 Eliska Pirkova, 'The Digital Services Act: your guide to the EU's new content moderation rules,' AccessNow (July 2022), https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/; and Asha Allen and Ophélie Stockhem, 'A Series on the EU Digital Services Act: Due Diligence in Content Moderation,' *Center for Democracy & Technology* (August 2022), https://cdt.org/insights/a-series-on-the-eu-digital-services-act-due-diligence-in-content-moderation/.

249 See for example: a joint civil society open letter led by Amnesty International, 'EU member states urged to curb invasive internet practices' (March 2022), www.amnesty.eu/news/eu-member-states-urged-to-curb-invasive-internet-practices/; the Tracking-Free Ads Coalition, accessible here: https://trackingfreeads.eu; European Data Protection Board, 'Statement on the Digital Services Package and Data Strategy,' EDPB (November 2021), https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf.

250 Dan Milmo, 'Molly Russell coroner calls for review of children's social media access,' *Guardian* (October 2022), https://www.theguardian.com/technology/2022/oct/14/molly-russell-coroner-calls-for-review-of-childrens-social-media-access.

Legislators and regulators may well need to expand tools to address negative social impacts and violations of fundamental rights from surveillance advertising in the future. Locking in handcuffs on regulatory powers through the back door of a trade agreement is inconsistent with the objectives of the EU. These are crucial issues of fairness and fundamental rights and should not be trade issues at all.

On liability, the DSA aims to set rules for tech companies to ensure they crack down on illegal speech and products and are more transparent about how they handle content. The Act will also help tackle harmful content which, like political or health-related disinformation, does not have to be illegal and introduce better rules for content moderation and the protection of freedom of speech.

However, there are provisions in digital trade agreements of the U.S. which copy Section 230 of the U.S. Communications law, which limits liability of platforms for harms caused by the activities of third parties on their platforms. While this provision is not part of the EU digital trade regime, it appears unbracketed in the latest iteration of the digital trade agreement under negotiation at the WTO.[251] Thus, holding platforms liable for harms caused by content on their platform may not be possible in the future, depending on the outcome of those negotiations.

## DMA[252]

The EU has been the leader in enforcement of competition policy against anti-competitive behaviours of Google, Facebook, and other U.S.-domiciled behemoths.[253] Now the EU is moving from enforcing fines against monopolistic behaviour, to banning several of the anti-competitive practices of online "gatekeepers" through the DMA.

The new rules outlaw certain abusive practices for which Big Tech companies have come under fire in the past, such as combining user data from a number of different sources without explicit consent and available alternatives. New requirements mandate operating systems to open up to third-party apps — giving iPhone users, for example, more flexibility in deciding what programs to install on their phones.

Moreover, interoperability rules that will allow users to communicate across different messaging services, such as WhatsApp and Signal, have been widely lauded by consumer organizations.[254] Big Tech corporations like Apple, Amazon and Facebook, including through their lobby DigitalEurope, have lobbied against this new legislation, but now they will be forced to comply.

A core provisions of the DMA mandates that business users of a platform must have access to the data that they generate in their use of the gatekeeper's platform. This would likely require the cross-border transfer of the data from the gatekeeper, say Amazon, to the business users, such as a European SME. This is a key step in levelling the playing field between Big Tech behemoths and SMEs which depend on these large marketplaces to operate.

But digital trade agreements explicitly bar states from being able to limit cross-border data transfers, or from mandating that copies of the data sets be held locally. It is unclear how the requirements that platforms disclose data to business clients could be enforced if a platform were to use its data rights under a digital trade agreement as a defence against forced data access or data sharing.

## DATA GOVERNANCE ACT (DGA)

According to the European Commission, the DGA is "a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes."[255] Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the GDPR applies. In addition to the GDPR, inbuilt safeguards are meant to increase trust in data sharing and re-use, a prerequisite to making more data available on the market.[256]

251 'WTO Electronic Commerce Negotiations Updated Consolidated Negotiating Text – September 2021,' WTO INF/ECON/62/Rev.2 (September 2021): 23 (see Article B.1(2) Interactive computer services (limiting liability)), available at https://www.bilaterals.org/?-other-292-.

252 European Commission, 'The Digital Markets Act: ensuring fair and open digital markets,' EU website, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en. Text of legislative resolution is available at https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_EN.html.

253 European Commission, 'Antitrust: Commission opens investigation into possible anticompetitive conduct by Google and Meta, in online display advertising,' press release (March 2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1703.

254 European Consumer Organisation, 'Crucial rules to rein in Big Tech and boost consumer choice to now become EU law,' European Consumer Organization (BEUC) press release (July 2022), https://www.beuc.eu/press-releases/crucial-rules-rein-big-tech-and-boost-consumer-choice-now-become-eu-law.

255 European Commission, 'Data Governance Act explained,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

256 Ibid.

The DGA "will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills."[257]

The DGA appears aimed to create a European data-driven economy. As such, it appears to have the potential to foster the use of data in the public interest.

However, in addition to fostering the re-use of public sector data for the private use, including by data trusts and data cooperatives as well as by Big Tech,[258] there do not appear to be provisions for requiring the sharing or re-use of private data (such as that held by Big Tech) for the public interest, an idea that may be required in the future. However, this public interest requirement could be constrained by "digital trade" rules that bar governments from being able to require data disclosures, subject to the weak general exceptions.

## DATA ACT (DA)

A proposal for a new DA was introduced in February 2022, with the intention of providing harmonized rules on access to and use of data. Along with the DGA, it forms part of the European Strategy for Data focused on European digital sovereignty.[259]

The DA proposal includes:

- Measures to allow users of connected devices to gain access to data generated by them, and to share such data with third parties to provide aftermarket or other data-driven innovative services.
- Measures to rebalance negotiation power for SMEs by shielding them from unfair contractual terms on data sharing, imposed by a party with a significantly stronger bargaining position.
- Means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency, such as floods and wildfires, or to implement a legal mandate if data are not otherwise available.
- New rules allowing customers to effectively switch between different cloud data-processing services providers
- New safeguards against unlawful data transfer.

One might wonder how this could be accomplished under EU digital trade rules that give the harvester of the data exclusive right to collect, transfer, store, use, sell, or utilize in whatever means they please, rights without the ability of the state to mandate practices like data sharing in the public interest.

## ARTIFICIAL INTELLIGENCE ACT (AI ACT) AND THE AI LIABILITY DIRECTIVE

The EU is also in the process of drafting an AI Act[260] with the stated goal of "making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy."[261] The AI Act would use a risk-based approach, banning certain uses of AI as unacceptable, and restricting the use of high-risk AI systems, while regulating limited or low risk AI systems. It is an effort to boost EU leadership in the field to take advantage of AI's benefits, while curbing unlawful surveillance or violations of fundamental rights.[262] Although it will be an improvement on the current lack of regulation, human and civil rights groups have found that the AI Act does not go far enough in protecting life-saving access to public benefits and services[263] as well as in protecting fundamental rights and offering rights of redress.[264]

257 European Commission, 'European Data Governance Act,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.
258 Collington, 'Digital Public Assets,' Common Wealth (2019).
259 European Commission, 'A European Strategy for data,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
260 European Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence' and 'Annexes to the Proposal,' European Commission COM(2021) 206 final (April 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206&from=EN.
261 European Commission, 'A European approach to artificial intelligence,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.
262 European Parliament, 'Artificial intelligence: MEPs want the EU to be a global standard-setter,' European Parliament plenary session ITRE press release (May 2022), https://www.europarl.europa.eu/news/en/press-room/20220429IPR28228/artificial-intelligence-meps-want-the-eu-to-be-a-global-standard-setter.
263 Human Rights Watch, 'How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers,' HRW Q&A (November 2021), https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net.
264 Civil society statement led by European Digital Rights and endorsed by 123 other civil society organizations to the EU, European Parliament, and all EU member states, 'An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement' (November 2021) https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf.

But "[p]rospective regulation of ethical, trustworthy and human centric AI may however require some measure of transparency or even disclosure over machine learning code and algorithms either in the course of an authorization procedure for critical applications or for the purpose of exercising regulatory oversight," found an academic study commissioned by the Dutch Ministry of Foreign Affairs.[265]

Under the proposed EU digital trade rules barring requirements for source code disclosure, foreign defendants could potentially claim treaty rights against the forced disclosure of data sets and the source code used in the AI, rendering the directive difficult to apply to foreign, but not domestic, defendants. A study by European Parliament's Committee on International Trade (INTA) noted that "trade rules could considerably limit the EU's rule-making capacity in relation to trustworthy and ethical AI."[266]

It further concluded that the "adoption of a similar provision in an agreement that would also be binding upon the EU risks hampering current EU efforts to make regulate AI, such as regarding its transparency."[267] The study points out that the EU High Level Expert Group on Artificial Intelligence also devises transparency as one of the requirements AI should meet."[268]

Thus, to regulate the Big Tech and their use of algorithms, countries must preserve their existing regulatory space by not taking any binding commitments on source code disclosures. Not knowing what kind of algorithms will be developed in the future, this regulatory space is extremely important for all governments.

In September 2022, the EU published a draft AI Liability Directive that would update liability rules for the digital age. The EU stands in contrast to the U.S. approach, in which Section 230 of the U.S. Communications law limits liability for platforms for activities of third parties on their networks. Instead, the new AI Liability Directive would empower consumers harmed by AI by presuming that a company is responsible if it failed to comply with legal requirements or refused to disclose the relevant documentation that the AI Act requires.[269] From media reports, it appears that the directive would mandate disclosure of "the datasets used to develop the AI system, technical documentation, logs, the quality management system and any corrective actions."[270]

In addition, the liability waiver for platforms embedded in the provisions of the proposed plurilateral digital trade agreement at the WTO would bar states from being able to hold platforms liable for publishing content created by third parties. The U.S. itself found the general exceptions so inadequate that it proposed a particular provision in the draft text to specify that the "measures necessary to protect against online sex trafficking, sexual exploitation of children, and prostitution, such as U.S. Public Law 115-164, the 'Allow States and Victims to Fight Online Sex Trafficking Act of 2017', which amends the Communications Act of 1934, is a measure that is necessary to protect public morals."[271] This is the only waiver in U.S. law of the prohibition on liability of Section 230.

265 Kristina Irion and Josephine Williams, 'Prospective Policy Study on Artificial Intelligence and EU Trade Policy,' *Institute for information Law* (January 2020), https://www.ivir.nl/publicaties/download/ivir_artificial-intelligence-and-eu-trade-policy.pdf.
266 Michele Fink, 'Legal Analysis of International Trade Law and Digital Trade: Briefing Requested by the INTA committee,' *European Parliament* (November 2020), https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2020)603517.
267 Ibid: 13.
268 European Commission, 'High-level expert group on artificial intelligence,' EU policy website, https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.
269 Gian Volpicelli and Samuel Stolton, 'EU wants to empower courts, victims in fight against harmful AI,' *PoliticoPro* (September 2022), https://subscriber.politicopro.com/article/2022/09/eu-wants-to-empower-courts-victims-in-fight-against-harmful-ai-00057225.
270 Luca Bertuzzi, 'LEAK: Commission to propose rebuttable presumption for AI-related damages,' Euractiv (September 2022), https://www.euractiv.com/section/digital/news/leak-commission-to-propose-rebuttable-presumption-for-ai-related-damages/.
271 'WTO Electronic Commerce Negotiations Updated Consolidated Negotiating Text – September 2021,' WTO INF/ECON/62/Rev.2 (September 2021): 24 (see Article B.1(2) Interactive computer services (limiting liability) provision 7(b)), available at https://www.bilaterals.org/?-other-292-.

# 8.

# WHAT DIGITAL RULES ARE NEEDED?

Big Tech advocates commonly proffer the solipsistic argument that since there is a lot of digital trade, there must be rules governing this trade. Indeed, a lot of new rules are needed to govern Big Tech. The pandemic-induced accelerated use of online systems exposed the urgent need for innovative regulatory interventions in many areas. But the rules proposed by Big Tech would actually exacerbate, rather than constrain, their dominance over economic, social, and political life in Europe and around the world and the harms that dominance has wrought.

Instead, what is needed are efforts to: ensure human and fundamental rights in the digital economy; promote the use of data and digitalization for the public good; and promote digital industrialization.

All countries need data as a public good. All countries need to harness the value of data for the public interest, such as expanding access to quality public services, ensuring fairness and non-discrimination, and using data to assist in finding solutions to pressing social ills such as climate change. For example, public bodies should have rights to de-personalized privately collected data for public interest purposes, such from ride-share apps for transportation planning. Data should belong to and benefit the community which produces it, and not only the Big Tech firm that harvests it. What is needed is an effort to build a public data infrastructure for the public good.

"Data should be the fundamental public infrastructure of the 21st century, as were roads, street lights and clean drinking water in the past. As a partner on the Decode project, we want city governments to start reconceiving data as a new type of common good,"[272] said Tom Symons, co-author of "Reclaiming the Smart City: Personal Data, Trust and the New Commons."

One of the key strategies to use data and digitalization for the public good is digital industrialization, which would require rules and practices to promote innovative small businesses; foster job creation; prevent the roll-up of monopolies; ensure decent work and rights for workers in the digital sphere; and ensure communities benefit economically from digitalization. We need digital industrialization policies that benefit the majority, and that reverse the decades-long trend of capital capturing all of the gains of productivity growth.

This would require a different approach entirely from the rules championed by Big Tech, because it would require efforts to rein in Big Tech's power. A non-exhaustive, brief review of the new digital rules that are needed include:

- New tax rules to ensure that Big Tech pays its fair share.
- New anti-discrimination rules that address rampant discrimination and harms from AI.
- New liability rules to prevent corporations from profiting from harm.
- New cybersecurity rules to prevent repeated leaks and hacks.
- New rights for gig workers – and existing workers' rights applied in the digital economy.
- New anti-trust rules that break up the vertical integrated monopoly behemoths.
- New rules to improve competition policy and end monopolistic abuses.
- New rules to ensure that SMEs and start-ups have a fair shot in the economy.
- New data-sharing rules to promote data for the public good.
- New rules to make the digital economy more environmentally sustainable.
- Enforcement and strengthening of hard-won rules governing digital privacy and data protection.

272 Theo Bass, Emma Sutherland, and Tom Symons, 'Reclaiming the Smart City: Personal data, trust and the new commons,' *Nesta* (July 2018), https://www.nesta.org.uk/report/reclaiming-smart-city-personal-data-trust-and-new-commons/.

However, none of these can be delivered through a "trade" agreement. This is because trade agreements inherently limit states' rights to regulate economic behaviour, while providing rights to trade which are exercised by trading corporations. It is also because the trade negotiations machinery is more heavily weighted towards favouring business, over and above other public interest issues such as labour rights or privacy rights.

To accomplish these public interest goals, instead decisions must be taken through democratic channels involving legislators, regulators, technical experts, civil society, trade unions, and representatives of affected communities. The private sector is but one of those communities.

It has heretofore been the arbiter of nearly all decisions affecting the digital economy and digitalization more generally through the trade space. Their reign over decisions that affect the lives and rights of all must end. The digital trade agenda is an effort to constrain the ability of regulation in the public interest across the board.

Citizens and legislators must ensure that states maintain policy space for the above by NOT having "digital trade" agreements restricting it in the WTO or in bilateral agreements.

# 9.

# CONCLUSION

There is a tremendous amount of public debate on the negative impacts of the current lawlessness of Big Tech in the EU. Parliament and the Commission are debating and enacting further legislation right now which will fundamentally alter the regulatory landscape. Big Tech, and particularly US-domiciled corporations, are attempting an "end-run" around this deliberative, democratic process, by using "trade" policy to try to lock in handcuffs on the ability to regulate, on a permanent basis. Big Tech wants to lock-in their "rights" to control data, now and in the future, before governing bodies realize the vast value of that data. Using spurious justifications, they want to lock in secrecy mechanisms over the business practices – algorithms – that govern an increasingly vast number of decisions over innumerable aspects of human life, by banning requirements to disclose source code.

Who benefits from digitalization, like with any technology, will depend on the policy landscape in which the technology is utilized, and that will include global rules set in trade agreements.

In order for digitalization and data to positively impact, rather than harm, society and our shared environment, those policies must be shaped in the public interest. To do so, Big Tech's foreclosure of that policy space through "trade" rules must be prevented.

It could be advantageous for EU legislators, regulators, the media, and the public to take this under consideration when trade officials claim that the digital trade agenda is in their interest. Further investigations of the potential conflicts of these provisions and other existing trade rules with new EU laws, as well as with existing fundamental and human rights, are highly warranted.

# ANNEX - TABLE COMPARING KEY DIGITAL TRADE CLAUSES IN EU-UK AND EU-NEW ZEALAND FTAS

| | EU-UK TCA[i] | EU-NZ FTA[ii] |
|---|---|---|
| **Free flow of data and data localisation** | *Article 201*<br>**Cross-border data flows**<br>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 a Party:<br>(a) 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;<br>(b) requiring the localisation of data in the Party's territory for storage or processing;<br>(c) prohibiting the storage or processing in the territory of the other Party; or<br>(d) 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.<br>2. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of 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 paragraph 1. Such a request shall be accorded sympathetic consideration. | *ARTICLE 12.4*<br>**Cross-border data flows**<br>1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy and recognise that each Party may have its own regulatory requirements in this regard.<br>2. To that end, a Party shall not restrict cross-border data flows taking place between the Parties in the context of activity that is within the scope of this Chapter, by:<br>(a) requiring the use of computing facilities or network elements in its territory for data processing, including by requiring the use of computing facilities or network elements that are certified or approved in the territory of the Party;<br>(b) requiring the localisation of data in its territory;<br>(c) prohibiting storage or processing of data in the territory of the other Party; or<br>(d) making the cross-border transfer of data contingent upon the use of computing facilities or network elements in its territory or upon localisation requirements in its territory.<br>3. For greater certainty, the Parties understand that nothing in this Article prevents the Parties from adopting or maintaining measures in accordance with Article 25.1 (General Exceptions) to achieve the public policy objectives referred to therein, which, for the purposes of this Article, shall be interpreted, where relevant, in a manner that takes into account the evolutionary nature of the digital technologies. The preceding sentence does not affect the application of other exceptions in this Agreement to this Article.<br>4. The Parties shall keep the implementation of this Article under review and assess its functioning within three years after the date of entry into force of this Agreement unless the Parties agree otherwise. A Party may also at any time propose to the other Party to review this Article. Such request shall be accorded sympathetic consideration.<br>5. In the context of the review referred to in paragraph 4, and following the release of the Waitangi Tribunal's Report Wai 2522 dated 19 November 2021, New Zealand:<br>(a) reaffirms its continued ability to support and promote Māori interests under this Agreement; and<br>(b) affirms its intention to engage Māori to ensure the review referred to in paragraph 4 takes account of the continued need for New Zealand to support Māori to exercise their rights and interests, and meet its responsibilities under te Tiriti o Waitangi/the Treaty of Waitangi and its principles. |

i Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, Document 22021A0430(01), 01/12/2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.149.01.0010.01.ENG&toc=OJ%3AL%3A2021%3A149%3ATOC

ii EU-New Zealand: Text of the agreement https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en

| | EU-UK TCA[i] | EU-NZ FTA[ii] |
|---|---|---|
| **Protection of personal data and privacy** | *Article 202*<br>**Protection of personal data and privacy**<br>1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade.<br>2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application (34) for the protection of the data transferred.<br>3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains.<br>(34) For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases. | *ARTICLE 12.5*<br>**Protection of personal data and privacy**<br>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.<br>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.<br>3. Each Party shall inform the other Party about any measures referred to in paragraph 2 that it adopts or maintains.<br>4. Each Party shall publish information on the protection of personal data and privacy that it provides to users of digital trade, including:<br>(a) how individuals can pursue a remedy for a breach of protection of personal data or privacy arising from digital trade; and<br>(b) guidance and other information regarding compliance of businesses with applicable legal requirements protecting personal data and privacy. |

| | EU-UK TCA[i] | EU-NZ FTA[ii] |
|---|---|---|
| **Access to source code** | *Article 207*<br>**Transfer of or access to source code**<br>1. A Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party.<br>2. For greater certainty:<br>(a) the general exceptions, security exceptions and prudential carve-out referred to in Article 199 apply to measures of a Party adopted or maintained in the context of a certification procedure; and<br>(b) paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract.<br>3. Nothing in this Article shall affect:<br>(a) a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition;<br>(b) a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure;<br>(c) the protection and enforcement of intellectual property rights; and<br>(d) the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article 277 of this Agreement. | *ARTICLE 12.11*<br>**Transfer of or access to source code**<br>1. The Parties recognise the increasing social and economic importance of the use of digital technologies, and the importance of the safe and responsible development and use of such technologies, including in respect of source code of software to foster public trust.<br>2. A Party shall not require the transfer of, or access to, the source code of software owned by a person of the other Party as a condition for the import, export, distribution, sale or use of such software, or of products containing such software, in or from its territory.1<br>3. For greater certainty, paragraph 2:<br>(a) does not apply to the voluntary transfer of, or granting of access to, source code of software on a commercial basis by a person of the other Party, for example in the context of a public procurement transaction or a freely negotiated contract; and<br>(b) does not affect the right of regulatory, administrative, law enforcement or judicial bodies of a Party to require the modification of source code of software to comply with its laws and regulations that are not inconsistent with this Agreement.<br>4. Nothing in this Article shall:<br>(a) affect the right of regulatory authorities, law enforcement, judicial or conformity assessment bodies of a Party to access source code of software, either prior to or following import, export, distribution, sale or use, for investigation, inspection or examination, enforcement action or judicial proceeding purposes, to determine compliance with its laws and regulations, including those relating to non-discrimination and the prevention of bias, subject to safeguards against unauthorised disclosure;<br>(b) affect requirements by a competition authority or other relevant body of a Party to remedy a violation of competition law;<br>(c) affect the protection and enforcement of intellectual property rights; or<br>(d) affect the right of a Party to take measures in accordance with point (a) of Article 14.1(2) (Incorporation of certain provisions of the GPA) under which Article III of the GPA is incorporated into and made part of this Agreement, mutatis mutandis.<br><br>[1 This Article does not preclude a Party from requiring that access be provided to software used for critical infrastructure, to the extent required to ensure the effective functioning of critical infrastructure, subject to safeguards against unauthorised disclosure. ] |

| | EU-UK TCA[i] | EU-NZ FTA[ii] |
|---|---|---|
| **Customs duties on electronic transmissions** | *Article 203*<br>**Customs duties on electronic transmissions**<br>1. Electronic transmissions shall be considered as the supply of a service within the meaning of Title II of this Heading.<br>2. The Parties shall not impose customs duties on electronic transmissions. | *ARTICLE 12.6*<br>**Customs duties on electronic transmissions**<br>1. A Party shall not impose customs duties on electronic transmissions between a person of one Party and a person of the other Party.<br>2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on electronic transmissions, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement. |
| **No prior authorisation** | *Article 204*<br>**No prior authorisation**<br>1. A Party shall not require prior authorisation of the provision of a service by electronic means solely on the ground that the service is provided online, and shall not adopt or maintain any other requirement having an equivalent effect.<br>A service is provided online when it is provided by electronic means and without the parties being simultaneously present.<br>2. Paragraph 1 does not apply to telecommunications services, broadcasting services, gambling services, legal representation services or to the services of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority. | *ARTICLE 12.7*<br>**No prior authorisation**<br>1. Each Party shall endeavour not to impose prior authorisation or any other requirement having an equivalent effect on the supply of services by electronic means.<br>2. Paragraph 1 shall be without prejudice to authorisation schemes that are not specifically and exclusively targeted at services provided by electronic means, and to rules in the field of telecommunications. |

**The Left in the European Parliament**
Rue Wiertz 43 B-1047 Brussels
www.left.eu