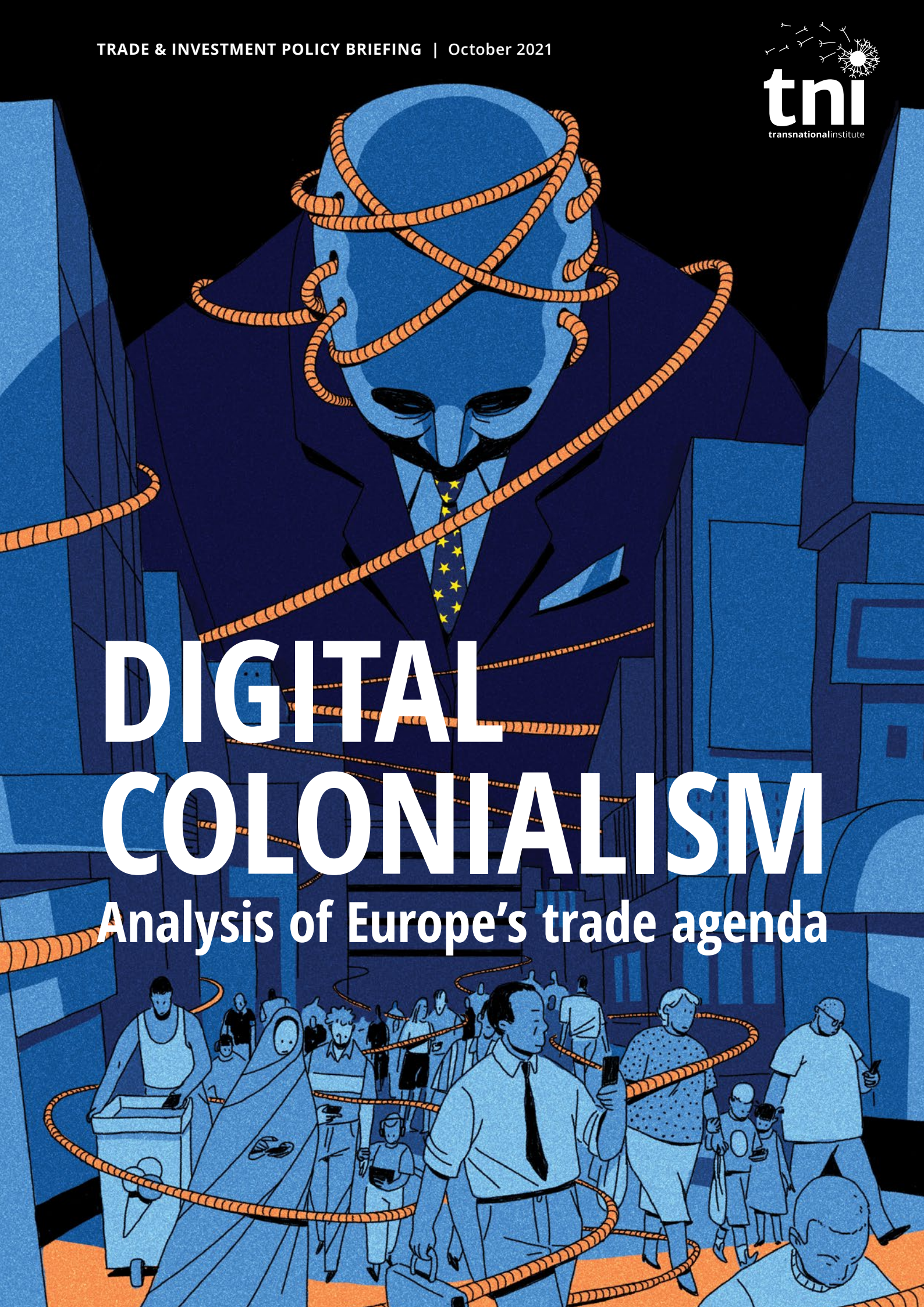
TRADE & INVESTMENT POLICY BRIEFING | October 2021

tni
transnationalinstitute



DIGITAL COLONIALISM

Analysis of Europe's trade agenda

Subscribe to our newsletter:
www.tni.org/en/subscribe

or scan the QR code:

AUTHORS: Sofia Scasserra and Carolina Martínez Elebi

EDITED BY: Nick Buxton

DESIGN: Evan Clayburg

COVER ILLUSTRATION: Anđela Janković

Published by the Transnational Institute, Amsterdam, October 2021

ACKNOWLEDGEMENTS: We would like to thank Adriana Foronda, Pablo Sanchez Centellas, Nick Buxton and Cecilia Olivet for their valuable comments on the text.

CONTENTS

EXECUTIVE SUMMARY

The global battle for control of the digital economy is typically portrayed as one fought by only two titans: US and China, but that does not mean that the EU has been standing still. As this briefing documents, the EU has been making strong efforts to catch up using trade negotiations and trade rules to assert its own interests. In the process, the EU is trying to climb up on the backs of the developing countries, undermining the chance for all to equitably share in the benefits of technological development.

This briefing examines 14 clauses on digital trade that the EU advocates for in its trade negotiations and their impacts on developing countries. Based on exhaustive analysis of 13 different EU free trade agreements as well as their positioning in the World Trade Organization, it shows that the EU has adopted a colonialist strategy, going out to hunt for data from the global South, in order to position its own companies in the new global cybernetic value chains. To empower its own Big Tech, the EU is seeking to force through clauses in trade negotiations that will hinder digital industrialisation, restrict necessary state oversight of corporations and undermine citizens' rights elsewhere, in particular in developing countries. While these clauses are technical in nature and obtuse to the general public, they can affect everything including peoples' rights to privacy, the nature and functioning of public services, the possibility of economic development and industrialisation, the accountability of government, even the quality of democracy itself.

DIGITAL TRADE CLAUSES

1. Measures that hinder digital industrialization
   a. Cross-border data transfer
   b. Prohibition on data localization
   c. Prohibition on local data processing
   d. Non-disclosure of the source code of software and related algorithms
   e. Elimination of customs duties on digital products and/or electronic transmissions
   f. Electronic public procurement
2. Measures that restrict needed state oversight of corporations
   g. Prior authorization
   h. Non-discrimination against digital products
   i. Electronic authentication and signatures
   j. Surveillance
   k. Liability of intermediary service providers
3. Measures that impact citizens' rights online
   l. Protection of personal data
   m. Online consumer protection
   n. Measures to prevent unsolicited electronic marketing communications

The battle the EU, US and China are waging is for control over the data we generate every time we connect to the internet as the basic raw material for its production process. The true value does not lie in the data itself, but from the processing of the data to deliver and sell algorithmic explanations of human behaviour.

The report shows that the EU was initially slow to advance its digital trade agenda, but has been much more aggressive since 2016. The EU appears to have two goals. First, to become a global digital player by creating rules that will support its industries transitioning to become digital ones, and which will then lock in their long-term dominance. These include fields as diverse as human resources, logistics, medical services, entertainment, education, and smart urban transport, although the most powerful push is coming from the EU's automative industry, keen to dominate the self-driving and smart cars of the future. Second, and particularly within WTO negotiations, the EU seems willing to prostrate itself to the power of the US digital giants, known as GAFAM (Google, Apple, Facebook, Amazon and Microsoft) who have spent a fortune in lobbying and succeeded in shaping any negotiations that include rules on the digital economy.

The EU has already signed six agreements that include clauses on digital trade, with Canada, Singapore, Vietnam, Mercosur, Japan and Mexico. It is currently negotiating a further seven agreements that include digital-related clauses with Tunisia, Chile, Indonesia, Australia, New Zealand and the region of Eastern and Southern Africa (ESA), and at the international level in the World Trade Organization. The negotiations underway with Indonesia, Australia, New Zealand and the region of Eastern and Southern Africa (ESA), together with the proposal presented by the EU to the World Trade Organization, are those that include the clauses most harmful to the countries of the global South.

The 14 trade rules summed up in the box are carefully designed to ensure that the big tech companies in the EU and the US can operate freely and maximise their profits in the digital economy, while restricting the ability of states to regulate the sector, redistribute the profits, improve their public services, or take forward a local technological development strategy. They also defund the state, by banning the collection of taxes on electronic transmissions, a huge potential future loss given the transition of everything online.

Even where the EU has been seen to be a more progressive player than China and the US, such as its adoption in 2018 of the General Data Protection Regulation (GDPR), exporting this via the means of trade rules will entrench rather than undermine an extractivist model. This is because it is not accompanied by the necessary resources to achieve it, which therefore creates additional costs for low-income countries and unfair competition.

The EU's digital trade agenda amounts to an agenda of extractivism. Mining raw material (data) from the global South without paying anything for it and taking it to the countries where they are based in order to process it and sell that technology back to us. It is also a strategy for the deliberate structural underdevelopment of low-income countries, as it seeks to put in rules that prevent them capitalising on the potential income and profits from technological development. Paraphrasing the well-known development economist Ha-Joon Chang, the EU's trade agenda is kicking away the digital ladder of development.

The losers in the battle for tech hegemony are ordinary people. Trade rules are not being constructed to strengthen citizen rights or democracy, but rather to benefit big tech, giving them markets and resources for free, unlimited monopolies and no social responsibility or tax liability. Against this resource theft and digital extractivism, the only remedy is to conserve the freedom of states to regulate so that people in turn can enforce their will. It it is therefore critical that states refuse to sign these agreements as a first step towards a longer-term process of digital industrialization and sovereignty.

1– INTRODUCTION

Though it seems like the distant past, it was not that long ago that our lives did not take place online and there were no records in real time of our social interactions or what we talked about or bought, the work we did or where we travelled.

The economy has rapidly become digital, and the COVID-19 pandemic has undoubtedly put the finishing touches to the merger of the online world with offline life. And if the online world has achieved one thing, it is to go undetected to the point where we no longer question it. We have naturalized it.

In recent decades, capitalism has started to mutate into a new phase as a result of these digital transformations: cyber-capitalism.[1] This efficient form of capital is slowly devouring the traditional forms. Thus, we find that in every sector of the economy there is a cyber or digital version of the same product or service, which is taking over the market and displacing traditional forms of production. Delivery apps now dominate the delivery business, taking over from traditional suppliers. Spotify sets the rules for the music market. Shippo organizes transnational logistics. Even the finance industry is starting to develop a cyber version in the form of cryptocurrencies.

This cyber-capitalism uses the data we generate every time we connect to the internet as the basic raw material for its production process.[2] The true value of cybercapitalism – which is creating extraordinary profits for the tech companies – does not lie in the data itself. As in any other production system, the raw material is the building block, but the vast profits do not come from there. **Profit is generated by processing that data to deliver and sell algorithmic explanations of human behaviour.**[3] What workers in the tech sector do is program algorithms that can process that data in real time and deliver or sell the final product to other companies. What is that product? The prediction of or explanation for how we behave and how we act. This is what is truly valuable in the economy of the future: processing data to obtain what some authors call the "behavioural surplus".[4] What the behavioural surplus amounts to is, first, to sell our behaviour as consumers; next, in a second stage, to sell our behaviour as citizens; and today, in a new phase of this cyber-capitalism, to sell and process our behaviour as workers.

Who is doing the selling? Who is doing the processing? Who is doing the programming? The big tech companies, commonly referred to by the acronym GAFAM (Google, Apple, Facebook, Amazon and Microsoft, among others). These companies began to accumulate data by developing various technology platforms and today they are the ones that determine the rules of the game in the digital economy. They are all US corporations, whose only global competitors capable of challenging their leadership are the tech companies in China, such as Alibaba or Tencent.

This digital economy is advancing in every sector and in every region of the world. Online sales are taking over from physical sales; traditional television – terrestrial or cable – is losing the battle against online content platforms such as YouTube or Netflix; online education and telemedicine are developing fast and becoming consolidated as new ways of providing essential services. As we increasingly connect to the internet in everyday situations, companies go undetected as they siphon our data, enabling them to find out our behaviours and preferences. The design of advertising and strategies developed from behavioural economics will continue to prescribe the reality in which we live. If an algorithm takes decisions about our lives based on all the information it has about us, it has the power to predict and determine our behaviour.

Although it may seem like science fiction, this reality is already happening and it will intensify and expand still further with the arrival of the 5G network and the Internet of Things (IoT), when a huge number of devices and sensors will be connected to the network and smart homes will monitor us 24/7. The fridge will know our tastes in food and be able to recommend purchases and offers, tell us when something is nearing its expiry date or when we are about to run out of milk, and even tell us that it is not healthy to eat a certain type of butter; the air conditioning will know what room temperature we prefer and adjust the settings so that the whole house is wonderfully warm (or cool) when we get home, and even suggest that we change the temperature in keeping with recommendations on electricity use. But they will also be able to demand that we pay more for receiving that service, or access our devices remotely if our behaviour does not suit their interests. A car insurance company will be able to order our vehicle not to move if, for example, our behaviour does not meet the standards it expects of us, or if we owe that insurance company money.

This cyber-capitalism is here to stay. The system that can be envisaged is one of mass surveillance, but also of structural under-development for most of the world's countries. Data extraction and technological development are basically taking place in two countries, by a handful of companies. They are carrying out historically well-known extractivist practices: mining raw material (data) from the global South without paying anything for it and taking it to the countries where they are based in order to process it and sell that technology back to us. This is nothing new. Indeed, it mimics the process experienced in the conquest of the Americas with the silver extracted from Potosí, or the sale of agroindustrial commodities from Latin America or Africa to be processed elsewhere so that the end products can be sold back. It is a system that weakens the terms of trade and impoverishes whole regions of the world. While this process is led by China and the US, all the other countries are gazing with awe at a technology that is difficult to understand. We are only now starting to realise the potential harm it can cause to our economies and democracies. Indeed, the widespread circulation of fake news, scandals such as Cambridge Analytica,[5] or the now proven manipulation[6] of voters by Facebook on election day[7] show how vulnerable our political systems are to outside interference by companies that ought not to have any influence on the fate of our nations.

We cannot give up on the dream of development. We cannot abandon democracy. We cannot relinquish privacy. Losing these things is not an unavoidable fate. There is another way of developing technology and using it to benefit the whole of society. There are alternative models that respect privacy,[8] and share out the economic benefits[9] among the citizens who produce the data and who are affected by technology. It is possible to imagine a type of state in which data is seen as a common good,[10] and that designs and develops good quality, more efficient, economically sustainable and culturally sovereign public services. To think of data as a private asset that can only be processed to earn profits for large corporations is to commodify our humanity: our geolocation, our communications, our society, our movements, tastes and customs cannot be seen as mere assets for private profit-making. If we declare data a common good, the economic benefits could be shared out more fairly in society and we could ensure that all those involved in producing a given data set are covered by the relevant privacy policy and able to use that data. A community should have the right to decide, how, why and for what purpose it wants its data to be used.

The big tech companies know that their profits depend on being able to continue to extract data and this is why they need rules that enable them to keep control. They need rules to entrench a business model that allows them to be the owners of cyber-capital, to guarantee them their monopoly over that behavioural surplus in perpetuity. Rules that enable them to eliminate competitors and establish themselves as the only future technological model. These rules are already written but the tech companies have not yet managed to get them approved everywhere in the world. We can see them in the negotiations going on in the World Trade Organization (WTO), but also in some Free Trade Agreements (FTA) that have already been signed, and others that are currently being negotiated.

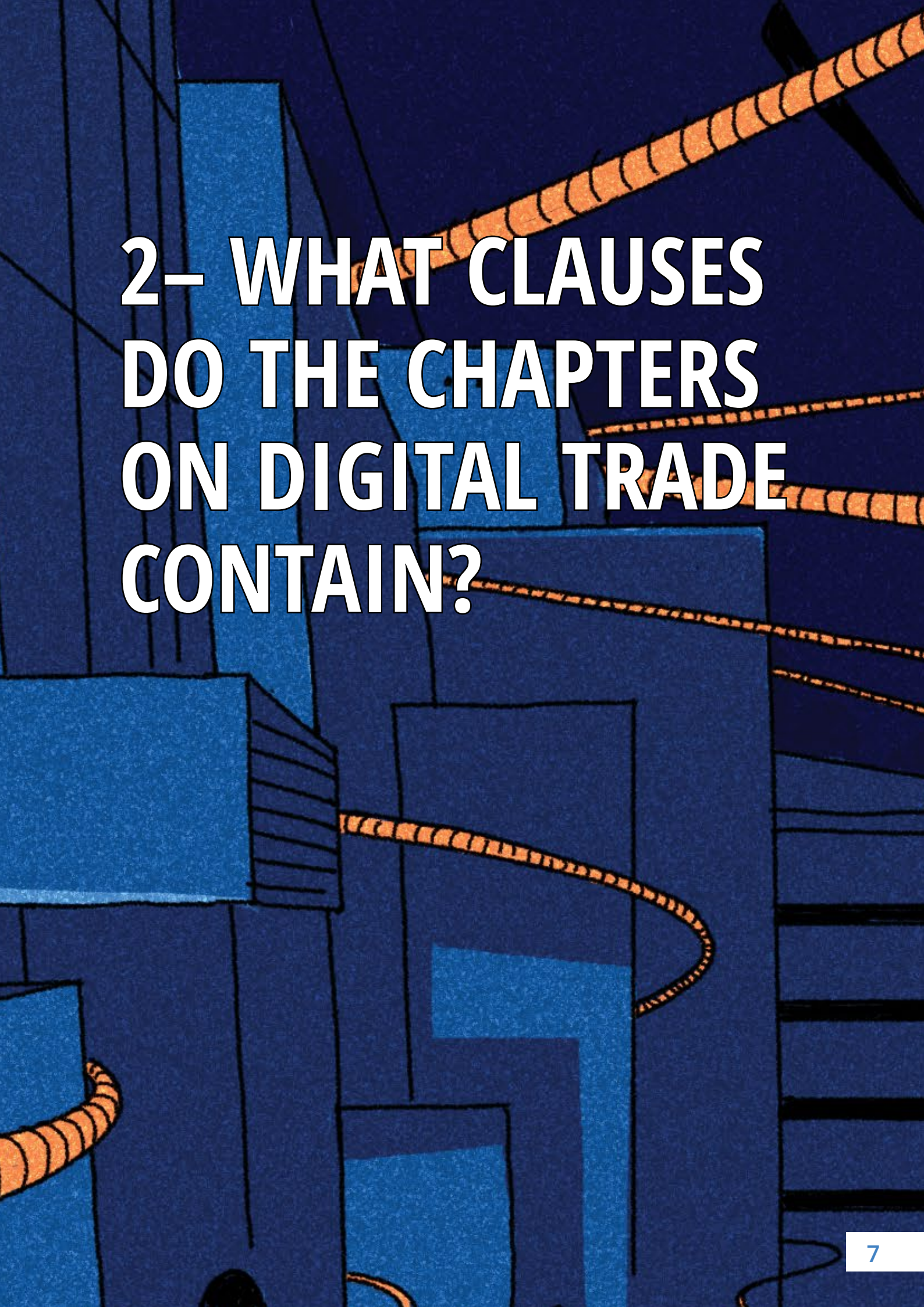
These rules are perfectly and carefully designed to ensure that the big tech companies can operate freely in the digital economy, but also to restrict the ability of states to regulate it, redistribute the profits, improve their public services, or take forward a local technological development strategy. But also, and above all, the aim of these rules is to defund the state, by banning the collection of taxes on electronic transmissions: if the economy of the future is online, restricting the collection of taxes on transmissions of this type is the greatest threat to tax revenue.

The award-winning economist Ha-Joon Chang warned in 2002 that "*Rich countries have 'kicked away the ladder' by forcing poor countries to adopt free market and free trade policies. Now-developed countries do not want more competitors to emerge as a result of the very same protectionist policies that they themselves successfully used in the past.*"[11] His statement today prompts us to reflect on whether the intention of this new free trade agenda might be to kick away the ladder to digital industrialization for developing countries. History is repeating itself.

The agenda on digital trade is not the only one to include clauses that relate to the digital economy. There are also agreements on finance and telecommunications that regulate the transfer of data in the sector, as well as computer services, but these were not included in this study.

In a world that is only just starting to understand the new digital economy and its importance, the most powerful countries, influenced by the big tech companies, have set the agenda for trade, writing rules that, if approved, will determine the future of our societies, our behaviour, and our lives.

It is crucial to know what is being negotiated and why it is important. We cannot afford to allow the handover of sovereignty and regulatory capacity in an area that is jeopardising our economies and above all our democracies.



2– WHAT CLAUSES DO THE CHAPTERS ON DIGITAL TRADE CONTAIN?

It was against the background of a geopolitical struggle for economic primacy and leadership in the development of Artificial Intelligence (AI) that clauses concerning the misnamed "electronic commerce" started to be timidly negotiated. The first discussions on the subject began in the WTO in 1998. To start with, it seemed to be just a trade issue concerning customs tariffs on goods and services sold online. But when we look at the clauses being negotiated today, it is clear that there is much more at stake. The rules governing the entire digital economy are being defined in these agreements.

First, it is useful to know that according to the WTO, *"Exclusively for the purposes of the work programme, and without prejudice to its outcome, the term 'electronic commerce' is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means"*.[12] In other words, practically all the goods and services produced in the economy today and in the future.

The now-classical ideology of "regulating to get rid of rules" became the dominant point of view. And while people in various forums pointed to the unbridled growth of the tech companies as a justification for regulating and enabling a fairer distribution of the profits, the text being promoted was written by and for the big tech companies.[13] Indeed, thanks to their lobbying, these companies have managed to include their demands in the negotiations. The rules basically give all the rights to the large transnationals, and only obligations and responsibilities to states. But above all, they handcuff states by limiting their capacity to regulate in order to steer the digital economy towards development objectives.

The European Union began later than the other developed countries to include some clauses on digital trade and data protection and use in the negotiations on bilateral free trade agreements and in WTO discussions on international trade. The EU's initial proposals sought to provide digital trade with a regulatory framework, but they did not include the more aggressive clauses favouring the corporations of the sort being promoted by the United States. But in 2015/2016 it became clear that the EU had changed tack. It started to include demands hitherto only pushed by the US. Why the change? What was the reason for this difference? Does the EU not know what it is negotiating, or is it seeking to benefit the GAFAM (Google, Apple, Facebook, Amazon and Microsoft)? The intention behind the negotiations is to develop tech services by siphoning data from the global South, just as in the past they mined precious metals and other raw materials. The aim of this digital extractivism is to build a critical mass of data that will make the EU a player in the global battle for technological power, through the development of new technologies such as self-driving cars, building on the large-scale automotive industry Europe already has.

Similarly, the US companies are engaging in frenetic lobbying[14] to attempt to ensure that European regulations do not harm their business. The tech companies, with Google at the forefront, have spent a fortune trying to influence any negotiations that include rules on the digital economy. Their aim is to get a set of rules at the national level and in the WTO that perpetuates their monopoly over technology.[15]

The clauses on the digital economy in the agreements that are being negotiated at the bilateral level by the European Union and at the multilateral level in the WTO shape the rules that will define cyber-capitalism in the future. These rules are at the heart of the system and reveal the interests that lie behind them, as well as the difficulties that periphery countries will encounter when they attempt to develop a digital industrialization strategy.

An exhaustive analysis of the most relevant clauses in the chapters[16] on "e-commerce" or "digital trade" being negotiated by the EU in its Free Trade Agreements (FTA) allows them to be grouped in three major categories.

The first column in the table below is the most harmful in terms of development for countries in the global South. These measures seek to entrench an extractivist model and defund states, as well facilitate a brutal competition that will hamper the development of incipient local technologies. The second column contains measures that limit the state's ability to control the companies operating online and moulding the digital market, giving the corporations rights and relieving them of duties. The third column includes measures that seek to remove protection from citizens and consumers, especially in the global South, by imposing requirements without transferring the resources needed to meet them. These are measures that exempt corporations from responsibility and affect the rights of citizens in digital settings.

Measures that hamper digital industrialization by countries in the global South	Measures that restrict state oversight of corporations	Measures related to citizens' rights online
Cross-border data transfer	Prior authorization	Protection of personal data
Prohibition on data localization	Non-discrimination against digital products	Online consumer protection
Prohibition on processing data locally	Electronic authentication and signatures	Measures to prevent unsolicited electronic marketing communications (spam)
Non-disclosure of the source code of software and related algorithms	Surveillance	
Elimination of customs duties on digital products and/or electronic transmissions	Liability of intermediary service providers	
Electronic public procurement		

The measures mentioned here are explained one by one in an exhaustive annex that includes the full text of the article in question, a detailed explanation of the debates around the problems they raise and clear examples to give an idea of the potential impact they would have.

3– THE EU POLICY ON DIGITAL TRADE

So far, the European Union has finalized six Free Trade Agreements that include one or more of the relevant clauses on digital trade. In addition, it is currently engaged in seven different negotiation processes on digital trade with countries in every region of the world.

However, not all the completed treaties or those under negotiation include the same clauses or EU requirements in the area of the digital economy (see Tables 1 and 2). These have changed over the years, as it became more relevant for the tech companies to outline rules that favour their business interests and protect their monopolies, as part of their strategy to continue as undisputed leaders of Industry 4.0 or the fourth industrial revolution.

Digital trade in completed treaties

An analysis of the clauses in the treaties signed by the EU to date reveals that the agreements with Mexico and Japan are the most dangerous in the area of the digital economy, followed by the agreement with Mercosur.

TABLE 1 – Finalized agreements with clauses on digital trade[17]

Clauses	Canada[18]	Singapore[19]	Vietnam[20]	Mercosur[21]	Japan[22]	Mexico[23]
Cross-border data transfer	NO	PARTIAL	NO	NO	PARTIAL	PARTIAL
Prohibition on data localization	NO	NO	NO	NO	NO	NO
Prohibition on data processing locally	NO	NO	NO	NO	NO	NO
Non-disclosure of the source code of software and related algorithms	NO	NO	NO	NO	YES	YES
Elimination of customs duties on digital products and/or electronic transmissions	YES	YES	YES	YES	YES	YES
Prior authorization	NO	NO	NO	YES	YES	YES
Non-discrimination against digital products	NO	NO	NO	YES	YES	YES
Electronic authentication and signatures	PARTIAL	PARTIAL	PARTIAL	YES	YES	YES
Online consumer protection	PARTIAL	PARTIAL	PARTIAL	YES	PARTIAL	YES
Measures to prevent unsolicited electronic marketing communications	PARTIAL	PARTIAL	PARTIAL	YES	YES	YES
Protection of personal data and privacy	PARTIAL	PARTIAL	PARTIAL	NO	NO	NO
Liability of intermediaries	PARTIAL	PARTIAL	PARTIAL	NO	NO	NO
Electronic public procurement	NO	NO	YES	NO	NO	NO
Surveillance	NO	NO	NO	NO	NO	NO
Year the negotiations started	2009	2010	2012	1999	2012	2016
Year the agreement was signed (or when the negotiations were finalized)	2016	2018	2015	2019	2018	2018

Negotiations on all these agreements started prior to 2016, and some, such as the negotiations with Mercosur, began in the 1990s. If there is one thing that stands out at first sight, it is that the free movement of data and its location, storage and processing were not seen as strategic issues at the time. This explains why these clauses were not included in the trade agreements.

Initially, the digital agenda consisted of maintaining the moratorium on customs duties on electronic transmissions. As the years went by, more and more regulatory issues were added to the agenda: regulating unsolicited emails, consumer protection, electronic signatures and authorizations, and

operating licences. Nevertheless, it is clear that this digital agenda was not as aggressive as that of the United States yet. The US had a strategy of digital colonialism towards developing countries through data extractivism since the digital revolution started.

It was only in the negotiations with Japan and Mexico that the first major controversial issue was introduced: non-disclosure of the source code of software and algorithms. The curious thing about the agreements that include it is to see how exceptions are added over time,[24] as problematic social impacts that could affect state sovereignty, public policy and national security come to light.

It seems that 2016 marks the turning point when the EU started to include new demands in the agreements, most of which have not yet been signed. Indeed, as they began to become more aware of what they were giving up by signing certain clauses, more countries started to put up resistance to the chapters on digital trade in the Free Trade Agreements (FTA). This coincides with the launch of the EU's new trade policy[25] and the subsequent approval (2016) and adoption (2018) of the General Data Protection Regulation (GDPR).[26] All these actions are in line with the 2016–2020 Strategic Plan drawn up by the European Union for trade-related negotiations[27] that include the digital economy as a priority and the new global demand in the area of trade in services.

The WTO Ministerial Conference in Buenos Aires in 2017 revealed this clearly. Most of the developed countries wanted to take forward an agenda on e-commerce, and sought to obtain a mandate for negotiations so that their agenda could be advanced at the next Ministerial Conference which was due to be held in Kazakhstan in 2020. Resistance from less developed countries, especially the Africa bloc, meant that no further progress was possible and prevented the mandate for negotiations from being approved. Some countries seem to understand what they would be giving up, or at least that they would be giving access to an essential raw material that they do not yet know how to process. Handing over this raw material in perpetuity did not seem to be the right strategy. What would happen if one day they figure out what to do with it? They would never again have access to it, and without having been given anything at all in exchange. But this is not all: they would also be conceding the right to negotiate new issues without having settled issues still pending from the past. Indeed, the Doha Round is still open and developing countries are still hoping for a historic overhaul of the rules on trade in goods and services that would enable them to develop before placing new issues on the agenda.

What motivated the EU to change its strategy on digital trade in 2016?

Prior to 2016, the European Union had seemed like just another onlooker in a process that was beyond it, but that year everything changed. The negotiations on free trade agreements that began then, and have not yet concluded, included new demands that sought to advance its digital industry to enable the EU to become a player in the economy of the future.

The battle between China and the US over 5G looks like it will leave Europe trailing behind in terms of providing network infrastructure. However, the battle over the services that will enable the new network to operate may place the continent in a privileged position. The EU becoming involved in global value chains in an intelligent manner implies getting on board with the indiscriminate and colonialist digital extractivism that the big tech companies have been engaging in with everyone,

including the EU itself. Data accumulation enables the development of new services to be provided by manufacturing companies, and it seems that the EU wants to reserve that share of the market for itself. Manufacturing 'smart' fridges that can suggest that you buy things or alert you to special offers in your neighbourhood – herald new opportunities for profit and integration with other products and services (compared to a standard 'dumb' fridge. Yet it will only be possible to include all these services in industrial manufacturing if data is stored and processed.

Accordingly, this new digital capitalism whose main ambition is to accumulate data has been transforming the economy into what is known in all the international forums as the fourth industrial revolution, or Industry 4.0.[28] The EU, aware of having dropped the ball in the early stages of this revolution, began to change its strategy with the aim of getting involved in this cyber-capitalism by developing value chains based on digital extractivism from the global South to the global North. The European Data Strategy[29] clearly goes in this direction. The fierce lobbying[30] by the US tech companies in the region is what seems to have brought about this radical change in the agenda. The aim of this lobbying was to promote a liberal digital economic model, not only in trade relations but also within the EU itself, as the US tech companies attempted to avoid regulations that might limit their capacity to extract data in the European market.[31]

Digital trade in the treaties now under negotiation

In the last few years, the agenda has changed. New issues were included in the negotiations. The core digital agenda is present in the texts, and in the negotiations the clauses that refer to the free movement of data have been established as fundamental articles. Europe can be said to have understood digital capitalism, or at least realised that digital extractivism was the way to obtain a critical mass of data that would enable it to compete in the design of tomorrow's economy.

This becomes evident when the clauses included in the new negotiations currently under way are analysed.

Table 2: Agreements currently being negotiated with clauses on digital trade

Clauses	Tunisia[32]	Chile[33]	Indonesia[34]	Australia[35]	New Zealand[36]	ESA[37]	WTO[38]
Cross-border data transfer	NO	PARTIAL	YES	YES	YES	YES*	YES
Prohibition on data localization	NO	PARTIAL	YES	YES	YES	YES*	YES
Prohibition on data processing locally	NO	NO	YES	YES	YES	YES*	YES
Non-disclosure of the source code of software and related algorithms	NO	YES	YES	YES	YES	YES	YES
Elimination of customs duties on digital products and/or electronic transmissions	YES	YES	YES	YES	YES	YES	YES
Prior authorization	YES	YES	YES	YES	YES	NO	NO
Non-discrimination against digital products	YES	YES	YES	YES	YES	YES	YES
Electronic authentication and signatures	YES	YES	YES	YES	YES	YES	YES
Online consumer protection	NO	YES	PARTIAL	YES	YES	YES	YES
Measures to prevent unsolicited electronic marketing communications	YES	YES	YES	YES	YES	YES	YES
Protection of personal data and privacy	NO	NO	PARTIAL	PARTIAL	PARTIAL	PARTIAL	PARTIAL
Liability of intermediaries	YES	PARTIAL	NO	NO	NO	NO	NO
Electronic public procurement	NO	YES	YES	NO	NO	NO	NO
Surveillance	YES	NO	NO	NO	NO	NO	NO
Year the negotiations started	2015	2017	2016	2018	2018	2019	2019
Year the negotiations were finalized	Paused in 2019						

**Only applies to Mauritius, the Seychelles and Zambia*

The proposed agreement with Tunisia is the only one that does not include the core elements of a digital trade agenda, and the negotiations on it have been at a standstill since 2019. If the negotiations are ever resumed, it remains to be seen whether the decision will be taken to include these problematic clauses.

4– CONSEQUENCES OF THE EU POLICY ON DIGITAL TRADE FOR THE GLOBAL SOUTH

What is at stake here is having the freedom and the sovereignty to develop a digital industrialization strategy, as opposed to a strategy of digital colonialism that relegates entire regions to being mere consumers of technology. With the worldwide rollout of 5G and the Internet of Things, it is expected that the electrical appliances we use every day will be able to generate data that will be analysed, leading to new services. Smart cars, for example, will not only take us around, but also advise us to get the vehicle serviced, tell us where we can get that done locally, and notify us when something goes wrong. If all this data is transferred to and stored in the European Union, that is where the new, more productive jobs will be created in sales and marketing for the new advertising and prediction products.

Now, what does the EU gain if these agreements are approved? The main advantage is the ability to process data and develop those new services within the borders of the EU, which means new EU exports to periphery countries. At this stage of the game, it will be nigh on impossible for the EU to take over data processing and the development of artificial intelligence from giants like Google, but it can dream of getting the corporations to set up operations in EU territory to store, process and deliver data that describes behaviour and can be sold to other companies that will use it to develop new digital services.

At the same time (and this point is no less important), with the arrival of self-driving cars in the world market, European car manufacturers will be able to control the data these cars generate and continue to operate these super-productive services to control vehicles through the “brain” and sensors installed in the cars.

An entire data processing industry is developing, in fields as diverse as human resources, logistics, medical services, entertainment, education, and smart urban transport. Keeping control of the data is a way to allow local European companies to grow at the cost of an increasingly subjugated global South, which will sell commodities in exchange for consuming everyday technologies, with ever weaker terms of trade.

In short, data will continue to be taken in an extractivist fashion without leaving any kind of revenue, and without even allowing countries to collect customs duties on imported digital services. This is a perverse result for the majority of the world’s people.

Europe’s position on this issue in the FTAs works in its favour and against less developed countries. But on the global scale in the WTO, Europe’s agenda works in favour of the large US corporations collectively known as GAFAM (Google, Apple, Facebook, Amazon and Microsoft) and against China. Should the regulations be approved multi- or plurilaterally in the WTO, they would be much more wide-ranging, and Europe would lose the ability to extract data from the global South and be forced to compete with the US corporations. There is no doubt that US capacity to absorb data is infinitely larger than Europe’s.

Online surveillance, consumer protection, authorization to operate, public tenders: all these measures seek to enable European firms to access markets to the detriment of small local companies that may be starting up in developing countries. Europe is aiming to expand its extractivist investments in countries in the South by positioning its companies as undisputed leaders in a market that used to be industrial and has now become dominated by cyber-capital.

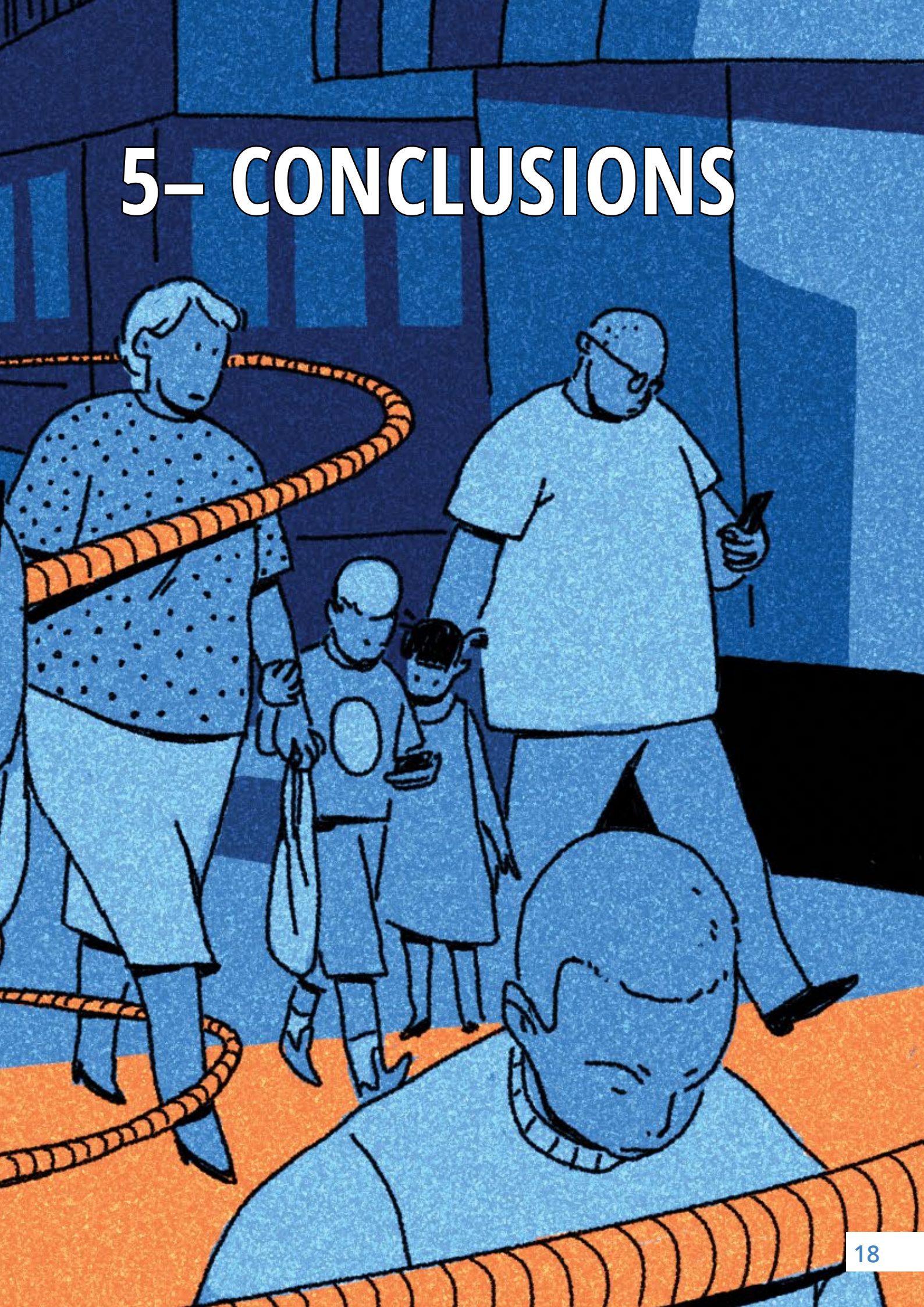
Europe has certainly understood that cyber-capital will take over from industrial capital in the future. Getting on board with the free digital trade agenda will enable the companies it has today to make the technological leap forward and turn themselves into major corporations that develop their own digital services instead of having to outsource those services to US corporations. Given that each sector has to develop its own cyber-version, having that version provided from outside is not the same as developing it endogenously within the company itself. Europe seems to be laying the groundwork for this strategy on behalf of its companies, so that they can go out and compete in the global market, gain consumers in under-developed and emerging markets, and conserve their export capacity. It is a model for corporate survival based on extractivism and the under-development of the majority.

This agenda is being pushed in various forums, using excuses such as promoting small and medium enterprises or gender equality. There is a "pink washing"[39] of the e-commerce agenda, arguing that women will be able to find better jobs online, selling products and becoming exporters on digital platforms.[40] In reality, women globally have less access to the internet,[41] and when they do have it they tend to use the tool in less economically productive ways.[42] Moreover, exporting not only implies having internet access but also requires infrastructure and skills to overcome the barriers of language, IT, tax and standards, to mention just a few. The true impact will be more under-development in the majority of the world's countries so that a handful of women in developed countries can turn themselves into exporters. There are strong evidence to suggest that the e-commerce agenda will widen the gender gap.[43] Indeed, several women's organizations have already expressed their opposition to the digital trade agenda.[44]

It is also argued that SMEs will benefit from the opening up of international markets, allowing them to sell their products. With the international trade rules proposed here, it is clear who will be the main winners in global trade. Small and medium enterprises in periphery countries will be displaced when they have to compete with the indiscriminate entry of products from abroad in their local markets.

The agenda does open the door to participation in an increasingly dynamic economy, but it does so at the cost of depriving many countries in the global South from having that opportunity. Inside the EU, it benefits transnational tech companies and large local industrial corporations that pursue the digital transformation. The people continue to be left behind, with no possibility of having digital sovereignty, dependent on consuming tech outputs produced with an extractivist logic and the clear objective of maximizing profits over and above the sustainability of life.

5– CONCLUSIONS



For years, Google, Apple, Facebook, Amazon and Microsoft (GAFAM) have attempted to push this agenda in free trade agreements and other multilateral forums where trade rules are established. The partial success they have had so far shows that the entire world trade system is systematically aligned against the interests of less developed countries. As they are required to negotiate new issues, the old trade agenda issues – such as farm subsidies – are left unresolved, awaiting a favourable outcome for those countries that export commodities.

At the beginning of the 2000s, there was no noticeable resistance to trade negotiations on the digital economy, but as time has gone by, more and more countries are becoming aware of the importance of recognizing the value of data as a commodity. Understanding its economic value has gradually led to greater resistance to negotiating agreements on e-commerce. Nevertheless, the efforts being made to disguise this agenda are truly disconcerting. Arguments such as "if we don't negotiate, inequality will worsen," "the digital economy is the future and we urgently need rules for it," and "it benefits SMEs and women – we should not deprive them of the opportunity"[45] resound in the corridors of the World Trade Organization (WTO) and the various other places where agreements of this type are being promoted, pushing countries to negotiate an agenda that has nothing to do with achieving those objectives but quite the opposite: the aim is to have rules that prohibit other rules from being imposed. A digital liberalism tailor-made for the great powers.

The 2020 WTO Ministerial Conference in Kazakhstan was cancelled due to the Covid-19 pandemic, but that did not mean the negotiations ground to a halt. The agreement on the digital economy espoused by the "Friends for E-Commerce for Development,"[46] as the group of countries currently negotiating the agenda plurilaterally calls itself, is expected to be finalized very soon. The WTO began in 2021 with a new Director General, Ngozi Okonjo-Iweal.[47] The institution is led by a woman from Africa for the first time. While it is not clear yet her position, she has been facilitating the conversations around the e-commerce plurilateral agreement even she has no mandate to do so. Her appointment is nevertheless essential if the agenda is to advance given her role in facilitating discussions and promoting new issues. The Friends for E-Commerce group hope to make progress in the run up to the next Ministerial Conference in November 2021.

The European Union faces the challenge of fighting a battle that it has already lost: digital supremacy today is disputed between two countries, the US and China. The plan is, then, to start with a colonialist strategy, going out to hunt for data from the global South, in order to position its companies in the new global cybernetic value chains. Traditional industrial companies are evolving towards producing services aggregated through digital channels, and the options are either to produce them within European companies or to outsource these services to tech companies. The opening up of markets and positioning of European companies in other countries would facilitate digital extractivism and the cybernetic capacities of European companies. In addition, lobbying by US corporations in the EU has reached unprecedented levels, as they organize constant meetings in the attempt to convince European negotiators to sign up to the e-commerce agenda[48] they themselves designed.

But above all, Europe is not only playing an economic game but a political one too in the battle between China and the US. The debate has already impacted on companies like Huawei, which have sought to penetrate the European market by supplying devices for 5G. Some European countries have closed their doors to these investments, mainly as a result of pressure from the

US government.[49] It seems that Europe wishes to side with the reigning power against the rising one in this battle for supremacy. And the Asian giant has instead refocused on consolidating itself as the undisputed leader in Asia, the main investor in Africa and a strong influence in Latin America, gradually pushing out the Atlantic powers and depriving them of allies.

This strategy has its correlate in trade agreements, where the RCEP (Regional Comprehensive Economic Partnership)[50] has already been finalized, forming a trade bloc of unprecedented size in the eastern region of the world. A trade war between the two powers in Latin America has already been declared. The US' fear over China's rising influence in 'their backyard' can be seen in the recent lobbying by the US in the election for the president of the Inter-American Development Bank to limit China's actions in the region.[51] The US fear of Chinese companies' strategy in the region meant it was willing to break a historic pact with the region (since the agreement was that the president of the IDB was supposed to be from Latin America) to nominate a US citizen, Claver Carone in order to restrict the expansion of Asian investment in the region.

Europe has opted to continue with the model that has worked well for it so far: having the US as its staunch ally to strengthen a cross-Atlantic region that make smart business with Asia. The failed attempt to approve and sign the TTIP (Transatlantic Trade and Investment Partnership)[52] had that as its aim. Activism and resistance by social movements was key to prevent the consolidation of an alliance that would have led to the hegemony of the bloc, to the detriment of the weakest and at a cost to people's sovereignty and democracy.

The truth is that the rules of the digital economy have already been written[53] and they do not work in favour of ordinary people. They do not seek to strengthen governments and democracies. Instead, they were written for, by, and for the benefit of the big tech companies, giving them markets and resources for free, unlimited monopolies and no social responsibility or tax liability. Against this resource theft, this digital extractivism and this monopolistic practice, the only remedy is to conserve the freedom of states to regulate – for the sake of our economies, but also and above all for our sovereignty, our culture and our democracy. There is no possibility of creating a fairer world if the pockets of the most wealthy continue to be filled at the cost of production by the poorest and through commodity extractivism. Peace is impossible without social justice.

This stance is far from being anti-technology. Technology has always been an ally of humanity. Technology cuts across our societies and is the making of them. It is simply a case of believing that technological development is possible with a different logic, one that places human beings, wealth distribution, and the benefit of all at the centre of the design of the systems that will govern our lives in the future.

Unfortunately, refusing to sign these agreements is no guarantee that that kind of economy will develop, but it would definitely leave the door open for any country that dares to think another future is possible to have the capacity to build it. To sign such agreements is to condemn ourselves. Refusing to sign them is the start of a long and difficult possible history of digital industrialization and sovereignty. "Don't kick away our ladder to digital development" could be the new slogan. The aim is to allow developing countries a way to climb up those steps and is necessary, to eliminate pockets of poverty and inequality.

Europe's strategy can be summed up as an attempt to get involved in a world where there are vast profits to be made, but it is a dangerous card to play. It will condemn other countries to underdevelopment while allowing foreign corporations to mould their democracy and their economy without being able to regulate it.

In an uncertain world that is has not stopped unbridled capital accumulation and at time of shifting geopolitical power, keeping the capacity to regulate to protect citizens, cooperating to expand competitive new digital hubs and promote the elimination of tax havens, as well as ensuring that the real tech giants pay taxes wherever they earn their profits, is the most sustainable, democratic, inclusive and fairest path for everyone.

ANNEX: THE CLAUSES ON DIGITAL TRADE AND THEIR IMPLICATIONS

CROSS-BORDER DATA TRANSFER

What does it say?

The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy.[54]

What does this imply?

Digital extractivsm

This means that data – the raw material of artificial intelligence – and other new industrial revolution technologies can cross borders and the state loses access to them. It implies that any company that starts to do business in the territory with which the agreement was signed can extract local consumers' and citizens' data and take it to another territory with no restrictions of any sort. It is crucial to understand this: once data crosses a border, it is impossible to demand access to it or its repatriation because the country loses jurisdiction over it. It is the equivalent of any other physical asset we can think of – say a work of art or a precious stone: once it crosses the border, it will be very difficult or nigh on impossible for the country to get it back.

One of the key concerns of approving cross-border data flows (or transfer) is how it will affect the privacy of citizens, especially in the case of sensitive data such as health records. Bearing in mind the reality of the buying and selling of databanks in the healthcare industry, some countries, such as Australia, have strict privacy laws. Australia's privacy law is more difficult for the government to enforce when the company running the data storage servers is based overseas. This is why Australia's electronic health records system requires data to remain in Australia and be processed there. If indiscriminate cross-border data transfer were to be approved, Australia would no longer be able to protect the privacy of its citizens' health data. There are also concerns about how big data could be used, especially in the immensely lucrative healthcare industry (pre-paid medicine, private clinics, pharmaceutical industry, laboratories).[55] The European Union has a law that protects the privacy of its citizens' data, known as GDPR.[56] This raises the question of what would happen if the data is taken to other locations where there are no laws regulating these matters. The law provides for this eventuality and protects European citizens, giving it extraterritorial jurisdiction, and the EU says it is developing systems to ensure that the European data protection law can be applied everywhere in the world.[57] Nevertheless, better global audit and control systems need to be developed to verify whether citizens' privacy is respected worldwide. However, it is difficult to demand these same things from developing countries, as they do not have the same resources to be able to develop such systems, while institutional weaknesses mean that they often do not have a good law to protect the personal data of their citizens.

In terms of economic development, data mining provides the vital raw material for artificial intelligence, which under this rule leaves the territory and never comes back. It also provides the information that is relevant when designing a public policy. Think for a moment how valuable Uber's data would be for developing an urban planning policy in the transport system, or how useful the data gathered by Google Classroom during the Covid-19 pandemic would be to any country's Ministry of Education. Being able to demand access to data is vital for the design of future effective public policies.

PROHIBITION ON DATA LOCALIZATION AND PROCESSING

What does it say?

Cross-border data flows shall not be restricted between the Parties by:

a. requiring 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 localization of data in the Party's territory for storage or processing;

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

d. dmaking the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localization requirements in the Party's territory.[58]

What does this imply?

Removing the digital ladder of development

Data as a commodity has various stages in its value chain. Moving data across a border is equivalent to exporting that commodity. But data processing and storage are also fundamental components of the value chain. Processing and storage can take place independently of the export of the data. If we attempt to sum up this clause, we could say that it amounts to digital colonialism and economic dependence. When contracting digital service providers, a country could include contractual clauses in its public procurement system that require the data to remain in the country and for the state to be given access to it for the purpose of designing public policies or, in the future, its own systems to replace the service provider, achieve economic independence, and contribute to digital industrialization. It could also pass a law setting out minimum requirements for any company that invests in its territory. With this clause in free trade agreements, the ability to do that would be restricted. Some countries are currently making use of that ability, which is strongly resisted by the dominant lobbying groups.[59] The corporate actors argue that localization requirements could lead to abuses in access to data by states. They also argue that although these requirements protect domestic industry in the short term, they do not create competition with other countries and thereby end up acting to the detriment of the economy. In other words, the requirement for data to be located in the country itself goes against the interests of transnational corporations and makes it more difficult for them to compete against local companies.

Data localization is undoubtedly a strategic economic issue now and in the future, because having data servers nearby allows various things to happen. For example:

- Information systems can be swifter and more effective, because otherwise triangulation occurs. When a citizen uses a service and performs a search online, that request must "travel" to the server where the data is held, the request must be processed, and the answer must travel back to the customer. This takes a few milliseconds and is almost imperceptible to the general public, but with the arrival of 5G it will be vitally important.[60] For driving a smart car or conducting remote surgery, this delay cannot be allowed to happen because it could cost lives.
- Keeping data under the jurisdiction of the country producing it could also enable access to it to be requested for health reasons, national security or other reasons. It provides sovereignty over the data, allowing this strategic input to remain inside a country's borders and within reach of those who produced it. Today, if a government needs data from Google, for example, it has to ask the US State Department for permission, the State Department in turn asks Google for it and only then will it be shared.[61]
- It creates advanced technology subsystems within the economy, as a data storage and processing centre requires specialized staff to assemble and maintain it, the production of hardware and software to run it, fibre optic networks that reach it and, in many cases, even renewable energy to power it. Many companies are starting to invest in stand-alone energy systems for their data centres due to the risk involved in losing power as a result of a fault in the national grid, the cost savings that this can bring, as well to minimise the environmental impact.[62]
- Processing usually takes place at the site where the data is stored in order to avoid a double triangulation that makes the final delivery of the product slower. This point is key as well, because processing is where the capitalist digital economy is most profitable. Processing boils down to the algorithmic systems that process data in real time, involving a larger number of highly productive tech workers. A data processing centre requires engineers, programmers, mathematicians, and a whole range of highly skilled workers.[63]

Example

One of the key reasons for keeping data storage and processing local is security, especially in areas that could affect a country's national security. This the main reason why the United States requires all cloud computing service providers to store data from the Department of Defence within its own borders.[64] Another reason for maintaining localization is for a country to be able to enforce its own laws and avoid legal disputes being settled in international or foreign courts. The government of New Zealand requires all tax records stored in the cloud to be held in servers located in New Zealand itself. Failure to do so is a crime punishable by a fine. Cloud backup is allowed, providing that the primary commercial records are stored in New Zealand.[65] If the proposal to prohibit data localization is approved multilaterally through the World Trade Organization, we could also see the emergence of "data havens"[66] similar to the notorious tax havens: places where transnational corporations can store their data without having to respect security and data protection laws or abide by any constraints on data processing, and thus obtain the maximum

possible profit. These data havens already exist, but if the proposal were to be implemented globally it would make it even more difficult for states to combat them.

Furthermore, revenue from data processing and storage has been growing worldwide.[67] The income earned from having data stored in a country is growing exponentially. The US receives 59.6% of total global revenue from this service, Western Europe 20%, Asia-Pacific 10%, and the rest is shared between Africa, Latin America and Eastern Europe.[68] As this makes clear, the business of storing data in the public cloud is concentrated in certain regions with an aggressive digital extractivism strategy. However, the increase in revenue is not only happening at the state level but also within the corporations themselves. In the case of the Visa corporation, for example, 38% of its revenue now comes from data processing.[69]

NON-DISCLOSURE OF THE SOURCE CODE OF SOFTWARE AND RELATED ALGORITHMS

What does it say?

No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party.[70]

What does this imply?

Inequality, poverty, exclusion and unfair competition

To gain a broad understanding of this clause in free trade agreements, there are several concepts that need to be explained beforehand. First, what is an algorithm? Everything that happens in the digital economy is based on algorithms – they are what actually process the huge quantity of data we generate every day. Algorithms are instructions, mathematical equations, which process information and return a result, which might be maximization or an optimization (statistical prediction), an order, a decision or a menu of options. When we do a search online, an algorithm decides which results we see first; when we log into Netflix, an algorithm decides which films to offer us; an algorithm processes medical images and indicates how likely it is that a shadow is a tumour; an algorithm assigns orders to delivery drivers.

This is what is known as Machine Learning and Deep Learning, two types of technology in the field of artificial intelligence, and it is amply documented that it suffers from certain shortcomings that are difficult to rectify. The concept of algorithmic bias is key here. Algorithms have very significant built-in biases, and although they can be minimized, it is unlikely that they can be completely eliminated. To start with, algorithms are fed by data, but that data is categorized and separated arbitrarily. From the gender binary category to the choice of possible fruits and vegetables, the categories chosen for data input can be biased and leave entire groups of data unrecorded, meaning that they will not be taken into account by the algorithm. Data itself is burdened by histories of violence and discrimination. For example, it has been found that women Uber drivers in the US earn 7% less than their male colleagues.[71] This is not because they are worse drivers or lack the

ability to engage in small talk with passengers. Instead, it is because the general public tends to rate them more negatively than men for cultural reasons. Finally, there is a programming bias which is undoubtedly the most important. The decision about what is and what is not important for an algorithm is ultimately a decision taken by human beings. Cathy O'Neil offers a very clear example.[72] She posits that she has an algorithm in her head that decides each night what to cook for dinner. The variables it uses are nutritional value, what ingredients she has in the fridge, how much time she has to spend cooking and whether she is in the mood for it, what she ate at lunchtime, her family's tastes, etc. Her head processes all this and decides what to cook on that particular day. What would happen if her son were to take control of the algorithm? Nutrition would certainly be a secondary consideration and taste would take precedence, resulting in chips rather than grilled fish. Biases are numerous and they have a huge impact on society. If we add to this the fact that most of the algorithms we use every day are programmed in industrialized countries by white men with a certain socio-economic status and level of education, we run the risk that minorities, dissidents and women will never be taken into account. Indeed, only 22% of programmers worldwide are women. In the US, the largest economy in the industry, 67.7% of programmers are white, 19.5% are Asian and fewer than 13% are black or have other ethnic identities. Latinos are not even counted in the statistics.[73]

Now, why is all this important? Because the article clearly prohibits the publication of the algorithm and the source code. It should be clarified that for strictly technical purposes, the algorithm is the order given and the source code the instruction or how that order is designed to be carried out. The legal equivalent would be that the algorithm is the law and the source code the regulation.

In some countries, such as Argentina, software (the source code and executable file) is protected under the Intellectual Property Law, in the form of copyright. In such cases, even though this protection exists and pirated copying is illegal, for example, access to read the code is not prohibited. It might be prohibited if the code or algorithm was protected as a trade secret, as some companies do. In other countries, such as the United States and Canada, software is protected under the patent system. Patents give the right to the exclusive use of functionalities, algorithms, representations and other actions that can be carried out by a computer for 20 years. In the case of patents, in order for this exclusivity to be awarded, the code is also made public and no-one else can use that code for as long as the patent remains in force.

Without access, it is impossible to audit the software to find out what the problem is should something go wrong. The clause tends to include exceptions in the area of defence and national security, or if an algorithm is suspected to contravene the country's competition laws. It is undoubtedly difficult to put together a case demonstrating that the algorithm needs to be audited and that the exceptions do not take into account problems affecting the general public, as in the case of discrimination against workers or facial recognition technology, to mention just two examples.

It should also be made clear that even when the source code can be audited, it is hardly ever easy to find what the mistake is or identify the problem that has arisen. In many cases, algorithms are written automatically by Machine Learning, and they end up being illegible even to programmers themselves. It is also worth pointing out that open-source software programs[74] are usually more reliable than closed-source software,[75] and are therefore more socially beneficial for the reasons described earlier.

In conclusion, this is a problem that is very difficult to solve. Humanity is only recently beginning to address it and it may have multiple impacts on our societies. In future, it could give rise to discrimination, environmental problems, attacks on democracy, economic destabilization and other negative effects. Plainly, it does not seem to be a good idea to limit a state's capacity to address a problem that we are only just starting to become aware of and we still do not know how to solve. Non-disclosure of algorithms has been problematic for many years now. This is why countries have started to include more and more exceptions, even in free trade agreements.[76]

Example

Access to the source code can be requested in legal cases, such as infringement of a software program's copyright, or disputes regarding the accuracy of diagnosis and test results (for example, in the case of an allegedly drunk driver who wants to find out how accurate a breathalyser device is). Access is also needed to find out whether the system is creating or reproducing discrimination against certain groups. It may be necessary to access the code to study it and thus reduce its vulnerability to hacking (in electronic voting systems, for example, or those used in sensitive areas like health, security and public administration, critical infrastructure such as nuclear power stations, and others). One of the reasons governments might have to require access to the source code could be to verify compliance with a particular regulation. An example of this is the Volkswagen emissions scandal, when the car company used software to pass emissions tests while in reality their cars were polluting up to 40 times over the legal limit when they were being driven.[77]

ELIMINATION OF CUSTOMS DUTIES ON DIGITAL PRODUCTS AND/OR ELECTRONIC TRANSMISSIONS

What does it say?

The Parties agree that electronic transmissions shall be considered as the supply of services, and neither Party may impose customs duties on electronic transmissions.[78]

What does this imply?

The emptying-out and defunding of the state are evident in this clause

If there was one thing we saw during the Covid-19 pandemic, it was that many of the things we thought could never happen online have done just that. Online school, teleworking and telemedicine were the major changes, but others that had slowly been making headway in the market, such as online meetings and seminars, also surged ahead. With every new advance in technology, an increasing proportion of the economy is going to shift to the internet. Indeed, the 5G project plans to create smart cities, factories and homes, with machinery and home appliances run remotely from other countries.[79] In cities with driverless buses, the driver is likely to be an algorithm in a data centre in some faraway territory. 3D printers allow designs that are marketed online to be printed directly in the country that buys the design. This is opening up a whole new world in the export of digital services, displacing manufacturing exports.

Therefore, prohibiting customs duties on electronic transmissions implies not being able to collect taxes at the border for any of these services provided from abroad. It amounts to a future defunding of the state.

Although it is true that the clause does not prevent the collection of domestic taxes (such as value added tax), it does ban the collection of customs duties, revealing that the objective is not to offer lower prices to consumers but something else entirely. When taxes are in the form of customs duties, it is the state that collects them directly when products enter the territory and it means that domestic products are indirectly treated differently, as they are not liable for these taxes. It makes goods produced within the country cheaper than those produced outside it. Domestic taxes, in contrast, are collected by companies directly from the consumer and the company itself is responsible for transferring that money to the state. This has several positive results for transnational corporations. First, only those companies that have a sufficiently large digital infrastructure to be able to differentiate between the taxes in each of the countries where they operate will be able to increase their market share. It will be difficult for their smaller competitors to maintain such a structure and they will be more likely to make mistakes, thus losing competitiveness. Second, it gives corporations extra foreign currency which they can delay paying, allowing them to earn interest on those funds. Third and finally, national treatment rules mean that if transnationals are charged a domestic tax, that tax must also be levied on their local competitors. Economies of scale play a crucial role here, as it is very likely that local companies will not be able to compete with the low prices the transnationals usually charge and will end up losing their market share.

In an increasingly digital and globalized economy, not being able to collect customs duties on electronic transmissions means depriving the state of its main source of funding and its ability to achieve sovereign national digital industrialization, as local tech companies lose out to international competitors.

Although this rule is currently being negotiated in free trade agreements, it has already existed in the WTO for years, in the form of the Moratorium on Customs Duties on Electronic Transmissions (MCDET). This was agreed multilaterally in 1998, long before anyone could imagine the extent of the digital revolution, before smart phones existed and before social media changed the way we communicate and get information.

The MCDET basically replicates the clause on the non-payment of duties on electronic transmissions found in free trade agreements, but at the multilateral level. Since 1998 it has prevented developing and less developed countries that are net importers of digital services from charging customs duties on them. The moratorium has been renewed every year since then and it has never been possible to revoke it, creating a genuine loss of tax revenue for the global South.

The purpose of including this clause in free trade agreements is to ensure that in the event of the WTO moratorium not being renewed, the commitment is upheld by means of the range of FTAs that have been signed.

Example

Digital free trade will probably lead to more imports of goods and services with a high digital content into developing countries, rather than exports from them. Its proponents disguise their proposals arguing that they are necessary in order to unleash development through the power of micro, small and medium enterprises (MSMEs) that use e-commerce. But in order to engage in this trade, countries must generate and increase value capture from production. If digital trade expands before developing countries have improved their productive capacities and digital infrastructure, (such as improving physical infrastructure and interconnectivity and adopting suitable rules on privacy, data protection and economic data rights), developing countries will simply be opening their economies up still further to foreign imports.[80]

Global Financial Integrity notes that transnational corporations drained between $620 billion and $970 billion from developing countries in 2014, mainly by means of dubious business manoeuvres.[81] One example is Uber, which uses subsidiaries in Ireland and the Netherlands to register most of its revenue, while registering its intellectual property in the tax haven of the Bermudas, leaving the countries where that revenue is generated (from Kenya to the United States) without the ability to collect the relevant taxes.[82] The WTO protects these transnationals from having to pay customs duties, and they can use subsidiaries in tax havens to avoid paying local taxes.

A report published by UNCTAD includes a simulation exercise that shows that if this moratorium becomes permanent – meaning zero customs duties on electronic products and transmissions – there will be an additional increase in imports of these products by developing countries, while imports by developed countries would not be affected. In many cases, not all of the imports in this category are electronic transmissions. There are still some imports that are not transferred electronically, such as music CDs or physical books, for example. As the digitalization of products increases and consumers choose to buy an e-book or download music from a platform, more of these products will be included in the category of electronic transmissions. The increase in imports of products of this type which are currently in this category will be highest in absolute terms for China, followed by India, Russia and Brazil.[83]

PRIOR AUTHORIZATION

What does it say?

1. The Parties shall endeavour not to require prior authorization solely on the ground that the service is provided by electronic means or adopt or maintain any other requirement having equivalent effect.

2. Paragraph 1 does not apply to telecommunication and financial services.

3. For greater certainty, nothing shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a *legitimate public policy objective* in accordance with the right to regulate, general exception, security exceptions and prudential carve-outs.[84]

What does this imply?

Incapacity of the state to control market players

Examples of this are mostly found in the telecommunication and financial services sectors. States often require prior authorization before a service can enter the local market. This enables them to regulate the number of competitors there can be and the type of service they are going to provide. They have to meet minimum requirements and, in the case of telecommunications, they even have to bid in a spectrum auction before they can start offering mobile phone services. This principle seeks to prevent prior authorization of this sort being required for any service provided by electronic means, with the exception of the two sectors mentioned.

Example

This situation causes various problems. First, in many countries applications such as Uber and Airbnb have attempted to start operating in cities. The problems they cause are well known,[85] as are the restrictions placed on them in some cities around the world.[86] If these agreements were to be signed, it would make it difficult to require prior authorization for an app to start operating in a city, leaving it free to enter any market it wants. It is worth pointing out the provision covers all services provided in digital form, now and in the future. This means that when hitherto unknown technologies emerge in future, the country would be prevented from stopping the entry of companies that might damage the local economy or protecting local competitors in nascent industries.

The article states that exceptions can only be made for restrictions aiming to achieve a *legitimate* public policy objective. As tends to happen with agreements of this type, what is considered legitimate is not specified, and it is left to the interpretation of the judges in the WTO or other international tribunals, who tend to rule in favour of companies and against states.

NON-DISCRIMINATION AGAINST DIGITAL PRODUCTS

What does it say?

Strictly speaking, very few if any agreements have clauses expressly mandating non-discrimination against digital products. Nevertheless, this is implicit in all the agreements through the principles of market access and national treatment.

A free trade agreement, whether it be bilateral, plurilateral or the result of negotiations conducted at the multilateral level in the WTO, always includes these clauses that basically state that there can be no difference between one product and another when determining tariffs, subsidies, tax benefits or any other measure that alters the conditions of trade.

By including digital products in free trade agreements, the principles of national treatment and market access are being applied to all digital products, unless it is expressly stated otherwise in the exceptions.

Thus, a digital product cannot be treated any less favourably than other products covered by an agreement. Neither can it be discriminated against compared with the treatment given to products manufactured locally. Likewise, a country cannot restrict the markets in which digital products or those provided by electronic means can be offered.

What does this imply?

This regulation implies a loss of sovereignty to make decisions on how the States want the market for goods and services, especially public services, to be shaped.

As digital services advance, a larger number of services will be provided this way. Education, for example, used to be a service that was typically not tradable, especially in the case of primary and secondary schooling. States often protected these sectors as they were considered essential public services. The aim was to preserve their sovereignty, especially over the process of producing the education service. Given that education has changed since the Covid-19 emergency and is starting to be provided permanently though online platforms, is it an education service, a digital service, or both? Can a limit be imposed on the use of Google Classroom, for example?

In the WTO and various trade agreements, many countries protect their public services from the rules of national treatment and market access for reasons of national interest and sovereignty. But if it is a digital service, does it automatically become covered by these rules, preventing a government giving priority to a national platform over a foreign one?

These dilemmas are starting to arise in all sectors of the economy, given that IT is becoming mainstream in the economy as a whole. This places rights (such as to education and health) at risk and implies the indirect privatization of public services. Indeed, health care may be a non-privatized public service, but if the state subcontracts a company to run all its telemedicine, then the company concerned will have all the data and may introduce a commercial rationale into the service, thus indirectly privatizing health care. This can be avoided by signing a contract that sets out the rules under which the service is to be provided. But if this type of digital economy agreement were to be signed, it would restrict what that contract could contain.

The inclusion of digital products in free trade agreements implies that the rules of free trade would indirectly apply to all services produced in the economy so far, even if they are protected under the agreement. But it also implies that free trade rules would likewise apply to future services not yet created and that we cannot even imagine right now.

Example

In the GATT (General Agreement on Tariffs and Trade) and GATS (General Agreement on Trade in Services),[87] governments made sure to allow discrimination against products when public procurement was involved. This is because they often have recourse to it in order to promote local products, especially for cultural reasons or for the purposes of economic development. If the national treatment and most favoured nation rules were to be applied to digital products without exception, governments would not be able to give preference to e-books or educational materials produced locally for students in their state schools, for example.[88]

ELECTRONIC AUTHENTICATION AND SIGNATURES

What does it say?

1. The Parties shall not deny the legal validity of an electronic authentication service solely on the basis that the service is in electronic form.

2. Neither Party shall adopt or maintain measures regulating electronic trust and electronic authentication services that would prohibit parties to an electronic transaction from mutually determining the appropriate electronic methods for their transaction; or prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their electronic transaction complies with any legal requirements with respect to trust.

3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law. Such requirements shall be *objective, transparent and non-discriminatory* and shall relate only to the specific characteristics of the category of transactions concerned.[89]

What does this imply?

This clause is an attack on the security of citizens and consumers

Although at first sight this clause may seem logical and well thought out, the reality is that electronic authentication and signature systems, though quite reliable, are not immune from attacks and hacking.

Indeed, blind faith in IT systems, which sees them as neutral, reliable, safe and swift, is what has led to these technologies starting to operate in such a wide range of spheres in society, even when they are not recommended by specialists, as in the case of electronic voting.

In many cases, an electronic signature may not be secure. There should be an escape route that allows the state to regulate which types of contracts and agreements cannot make use of electronic documents, signatures or stamps. Likewise, there are different security standards. The world of IT may implement security measures that are extremely difficult to break, but there may also be lax standards that are easily bypassed. It is usually – though not always – the case that enhanced security comes at a higher cost.

This is why the article clarifies that in exceptional situations performance standards regulated by an accredited authority may be required, but the same article specifies that these must be objective, transparent and non-discriminatory. The use of adjectives of this type without defining what they are understood to mean is typical in free trade agreements. It is left to the judgement of an ad hoc tribunal, whose members are usually the same lawyers who defend the interests of corporations, to decide what is objective, transparent and non-discriminatory. This is why states do not usually make use of clauses of this sort for fear of reprisals and having to deal with hugely expensive lawsuits as a result of having recourse to the exceptions.

Example

One of the problems with how this article is worded in most of the agreements is that the parties to the agreement have to decide which authentication technology they will use. This problem can be seen clearly in the case of Visa and Mastercard, two of the dominant firms in setting standards, which implemented their "anti-fraud software" in their business networks for the stated purpose of ensuring that the payment system was safe. However, the National Retail Federation in the US called the plan a "near scam", and a legal challenge asserted that "the system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties."[90] Indeed, many corporations have been found to be lax in the way they handle customers' data, and this has led to identity theft and credit fraud (the Equifax data breaches in February and September 2017 are a clear example of this), or cyberattacks on oil and gas pipelines (as happened in April 2018 to Energy Services Group and to Colonial Pipeline in May 2021 in the US),[91] as well as other problems that cause economic losses to consumers and other damage. There is evidently a need for state regulation – with clear and precise guidelines – and the presence of an accredited authority to set the security standards for the technology used for authentication, including the possibility of defining those cases in which electronic technology cannot be used and other methods of authentication, signatures and stamps must be deployed.

ONLINE CONSUMER PROTECTION

What does it say?

1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers, inter alia, from fraudulent and misleading commercial practices when they engage in electronic commerce transactions. Consent shall be defined in accordance with each Party's own laws and regulations.

2. To this end, the Parties shall adopt or maintain measures that contribute to consumer trust, including measures that proscribe fraudulent and deceptive commercial practices. Such measures shall, inter alia, provide for:

    a. The right of consumers to clear and thorough information regarding the service and its provider;

    b. The obligation of traders to act in good faith and abide by honest market practices, including in response to questions by consumers;

    c. The prohibition of charging consumers for services not requested or for a period of time not authorized by the consumer;

    d. Access to redress for consumers to claim their rights, including as regards their right to remedies for services paid and not provided as agreed.

3. The Parties recognize the importance of cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to electronic commerce in order to protect consumers and enhance consumer trust.[92]

What does this imply?

This is another of those measures which are not bad in principle, but it remains to be seen how they are worded and applied in the agreements, as there are already drafts where these articles are much more problematic, such as in the TISA (Trade In Services Agreement).

In principle, the idea is a good one: to protect consumers and give them ways to claim their rights and demand compensation should problems arise. The question here is whether local consumer protection agencies lose jurisdiction over this issue. Although they are mentioned in the article that says it is important for them to cooperate, they are not given the jurisdiction to act in cases that cannot be resolved through electronic channels. This could be detrimental to consumers when they do not receive a direct response from the company, as the courts they can take their case to do not have the power to force the company to provide redress.

Example

Tech corporations have demonstrated a lack of responsibility and commitment as far as guaranteeing consumer protection is concerned. Every week we hear about yet another leak of sensitive personal data of millions of users and consumers of the services provided by big tech companies around the world, whether they be providers of messaging services, social media or business transactions. There have been leaks of passwords, credit card numbers, photos, etc. Furthermore, consumers have filed innumerable claims after discovering that data related to their use of products and services, from Bose headphones[93] to email[94] and sex toys,[95] has been sold to other companies, usually without the consumer's knowledge or consent. One well-known international scandal involved Facebook, when it was found that it had improperly shared the data of 87 million users with Cambridge Analytica,[96] which might have affected the result of the US elections in 2016. There is evidence that this also affected elections in other countries in Latin America, such as Argentina and Brazil.[97] In these cases, the problems faced by consumers are evident, as they are unable to claim their rights from global corporations that ignore their demands. It is also clear that there is a need for local consumer protection agencies to play an institutional and legal role, with the ability to get involved in such cases in order to protect consumers in their countries who have not been able to solve their problems by engaging directly with the companies through electronic channels.

MEASURES TO PREVENT UNSOLICITED ELECTRONIC MARKETING COMMUNICATIONS

What does it say?

1. Each Party shall endeavour to protect end-users effectively against unsolicited direct marketing communications. To this end, in particular the following paragraphs shall apply.
2. Each Party shall endeavour to ensure that natural and juridical persons do not sent direct marketing communications to consumers who have not given their consent.
3. Notwithstanding paragraph 2, the Parties shall allow natural and juridical persons which have collected, in accordance with each Party's own laws and regulations, a consumer's contact details in the context of the sale of a product or a service, to send direct marketing communications to that consumer for their own similar products or services.
4. Each Party shall endeavour to ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable end-users to request cessation free of charge and at any moment.[98]

What does this imply?

While this seems to be a measure against spam, in practice it will allow it when a consumer has already bought goods and services or when the company has "collected" the consumer's data legally. This means that if you make yourself known online as a potential customer interested in a certain product, companies are automatically authorized to send you as much publicity as they like. This is because the tech companies sell the data of potential customers to the companies that sell such goods, without the need for the consumer to have given their data to a particular company. Once your consumer profile has been identified, all the companies that buy that information can legally send you marketing communications.

Example

All of us who use social media are already experiencing this today. The huge quantity of advertising that appears on our computer screens has already become unmanageable. Looking to the future, following the installation of the 5G network and the development of smart home technology, electrical appliances will have screens recommending that we buy things, telling us about faults and giving us automatic warnings. These appliances will most likely be connected to our mobile phones and send the notifications there too. Nothing will prevent a constant deluge of advertising on our mobiles and in our homes, every time we switch on an appliance or go anywhere near the fridge. Allowing states to regulate this in future could defend us from unrelenting offers, advertising and rampant consumerism.

PROTECTION OF PERSONAL DATA AND PRIVACY

What does it say?

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

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

3. Each Party shall inform the other Party about any safeguard it adopts or maintains according to paragraph 2.

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

5. For greater certainty, the Investment Court System does not apply to the provisions in Articles 1 and 2.[99]

What does this imply?

Although it is absolutely correct to give the privacy of personal and non-personal data the importance it deserves, there is a tendency in various free trade agreements to allow each country's data security and protection standards to be analysed based on if they measure up to the other country's standards. Obviously, as almost always happens, it is very expensive and complicated for developing countries to meet certain standards, especially EU ones, in order to compete as equals in the digital age.

Data protection and privacy is becoming essential in this new industrial revolution, and the privacy standards currently required are not always the same as those set out in a country's laws. This means that various countries are not only required to update their legislation and adapt it to EU laws, but also to modernize their systems and invest their scarce resources in data protection and security. Of course, raising standards is a good thing, and demanding an agenda that goes in that direction is necessary, but what is also required is to accompany such demands with the assistance necessary to reach the desired standard.

This article affirms the importance of working on it, but it does not outline how less developed countries can be helped to have the capacity to guarantee it or offer any commitment to do so. In other words, there is no real commitment to this issue, but rather just a statement of interest. There ought to be a requirement to raise standards and minimum international standards to guarantee privacy should be established, while also providing less developed countries with resources and mutual assistance to reach those standards. Establishing a requirement without

providing the means to meet it can result in unfair competition, whereby countries that do not manage to meet the established standards are disqualified. This has already been seen with regard to other global standards, such as environmental ones: they are necessary and positive, but they carry a high cost for countries in the global South, most of which were not responsible for the global pollution produced in the past. They are required to meet CO2 emissions standards, even though more developed nations only managed to achieve their level of industrialization by polluting the environment without any type of control. Today, developing countries are required to invest in more expensive technologies in order to meet those international standards. The same thing may happen with data protection if this agenda starts to be made compulsory. The right way to go about this is not to include clauses of this type in free trade agreements but rather to take forward an agenda of cooperation in other international organizations.

It should be clarified that there are rules on data protection in other chapters of free trade agreements, such as those on finance. But these are not included in this analysis.

Example

The European Union's General Data Protection Regulation is a clear example of regulation in the area of personal data protection from the standpoint of protecting privacy as a fundamental right. The regulation stipulates that in order for the EU to be able to transfer personal data, its trade partner must pass an "adequacy test" to ensure that the data will be protected.[100] However, because the United States does not have a single set of rules governing data protection, but rather a series of local regulations that differ from state to state and from one industry to the next, the only alternative for there to be trade transactions involving personal data is for the EU to allow the US to include in its agreement the possibility of accepting that voluntary guidelines are sufficient to comply with the provisions of the free trade agreement. This is a matter that ought not to be dependent on being included in a trade agreement. If it continues in this direction, the decision would go against the system to protect the personal data and privacy of people in the EU in order to ensure that trade can take place between the two parties. However, as the experience with environmental regulations indicates, systems that depend on voluntary compliance by corporations have not achieved their stated objectives.[101]

ELECTRONIC PUBLIC PROCUREMENT

What does it say?

1. When conducting covered procurement in accordance with the chapter on public procurement, the procuring entity shall:
    a. Ensure that the procurement is conducted using information technology systems and software, including those related to authentication and encryption of information, that are generally available and interoperable with other generally available information technology systems and software; and
    b. Maintain mechanisms that ensure the integrity of requests for participation and tenders, including establishment of the time of receipt and the prevention of inappropriate access.

2. For each covered procurement, the procuring entity shall publish a notice of intended procurement, which shall be directly accessible by electronic means free of charge through a single point of access. The notice of intended procurement shall remain readily accessible to the public, at least until the expiration of the time-period indicated in the notice. The appropriate electronic medium shall be listed by each Party.

3. For each covered procurement, the procuring entity shall also promptly offer unrestricted and full direct access free of charge by electronic means to the procurement documents from the date of publication of the notice.[102]

What does this imply?

When a government launches a tender for the private sector to participate in a public investment project, it usually decides the conditions in which the information is provided and how the tender process will be conducted.

This article proposes that tenders should be conducted by electronic means, making the information accessible free of charge and with cybersecurity standards and formats in keeping with those readily available in the market. This obliges states to move all their procurement processes online, in order to make it easy for transnational corporations not based in the country to participate. Not allowing the government to charge for the procurement documents deprives the state of a source of revenue and is another way of favouring the private sector. By broadening access and increasing competition for public procurement contracts, the state will be less able to give preference to domestic companies. With more competition from international firms, local companies will be less likely to win the contract.

Example

Given that no exceptions are proposed in this paragraph, it seems that the intention is for this to be applied to all public procurement processes – in other words, purchases of all goods and services. This differs from what is stated in other free trade agreements such as the Trans-Pacific Partnership Agreement (TPP), which does not cover all goods and services. Moreover, by not setting a minimum threshold for the value, the article could cover contracts which, were it not for this agreement, could be reserved for local micro, small or medium enterprises, in order to promote the development of a domestic industry (such as purchases of books and stationery, for example).

LIABILITY OF INTERMEDIARIES

What does it say?

Liability of intermediary service providers: simple transmission

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the Parties shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
    a. does not initiate the transmission;
    b. does not select the receiver of the transmission; and
    c. does not select or modify the information contained in the transmission.
2. The acts of transmission and provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network.

Similar rules apply to the caching and hosting of information.[103]

What does this imply?

> Information intermediaries exist on the internet as in any other sector of the economy. Facebook is an intermediary of the information that its users post. Netflix is an intermediary that takes films produced in Hollywood (and other shows) and sends them to your electronic device.

In many cases, intermediary platforms are used to commit illegal acts. For example, there are Facebook groups selling wild animals in Argentina – an activity punishable under the law.[104]

This article acknowledges that intermediaries can be used for illegal purposes. This is why it exempts them from liability for the content they transmit unless they produced it themselves (e.g. a film produced by Netflix), or have the ability to select the information they are going to transmit, or have actively modified that information. This exemption from liability also covers the storage, caching and hosting of information. A court can require the service provider to terminate or prevent an infringement. Similar rules apply to the caching and hosting of information.

Exempting intermediaries from all liability is risky, bearing in mind that various platforms are used to commit crimes such as human trafficking,[105] trafficking in wildlife, arms or drugs, child pornography[106] and other serious crimes. However the ambiguous way the article is worded does not resolve fundamental issues of liability and accountability. If intermediaries were to be held liable for all the content they circulate through their platforms, this would include content that could be classified as "hate speech" or "fake news", for example. That could lead these platforms to censor their content beforehand, solely in order to avoid sanctions of any sort. Measures of

that nature could infringe everyone's right to freedom of expression and, in particular, the rights of global minorities, who need platforms such as Facebook, Twitter or YouTube as a space to express their claims, denounce abuses and circulate information that the mainstream media will not carry.

Accordingly, an article of this nature is right not to hold intermediaries liable for the speech that circulates on their platforms, in order to avoid infringing the right to freedom of expression, but it should specify which crimes they should be held liable for and have the obligation to prevent their platforms being used for.

Example

Google and Facebook control the vast majority of the information and news that gets circulated, and their algorithms decide what information we see and what we do not see. Their willingness to allow their platforms to be used to interfere in democratic processes demonstrates their glaring lack of interest in striking a balance between their power and their responsibilities. One of their aims in relation to digital trade negotiations is to ensure that they cannot be held liable for the content on their sites that is created by third parties, even when that content encourages violence, interferes in elections or causes other types of harm, as this is what these corporations make their profits from.[107] Nevertheless, due to the suspicions of deliberate disinformation on social media that arose after Donald Trump won the US presidential election of 2016, and continued throughout his term in office, in 2018 the FCC repealed the "Open Internet Order". Faced with a constant barrage of criticism,[108] YouTube, Facebook and Twitter eventually began to moderate their users' content to prevent the spread of "fake news" and "hate speech". The consequence of this was a fall in content from dissident organizations, critical discourse,[109] and information from minority groups.

SURVEILLANCE

What does it say?

1. The Parties shall not impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.

2. The Parties may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[110]

What does this imply?

This issue is hotly debated in various political and social circles. To what extent are the platforms responsible for the content uploaded to them? Do we want to give them the power to monitor what gets uploaded? There are differing opinions about this. Some argue that if they had that power, they could use it for the common good and remove hate speech or misogynistic abuse from social media. Others argue that removing such speech does not mean it will disappear from society; it will just be driven underground. They also point out that the platform would be given a very important power: to decide what is good and what is bad. What if they decide that internet activism, trade unionism, or a certain political or economic ideology is negative and therefore ought to be censored? Do we really want transnational corporations to have that power?

The article stipulates that the corporations are not obliged to monitor their networks, but it does not prohibit them from doing so. It also says that if the government requests assistance they should provide it. This could clearly lead to an attack on democracy and freedom of expression if an authoritarian government comes to power in the future.

ENDNOTES

1 Sai, Fabian Leonardo. 2019. Fragmentos de fragmentos: Vida psíquica, forma estética, potencia histórica. Revista Espectros, Año 5, Número 6. http://espectros.com.ar/numero-6-fragmentos-de-fragmentos-vida-psiquica-forma-estetica-potencia-historica-leonardo-fabian-sai/

2 Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism. Public Affairs.

3 Gurumurthy, Anita and Chami, Nandini. (2020) *The Intelligent Corporation: Data and the digital economy* https://longreads.tni.org/stateofpower/the-intelligent-corporation-data-and-the-digital-economy

4 Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism.* Public Affairs.

5 https://en.wikipedia.org/wiki/Cambridge_Analytica

6 The idea of "direct manipulation" is what the media were attempting to argue at the start of the Cambridge Analytica scandal (similar to the theory of communication known as the "hypodermic needle theory"). After the case was studied in depth, it was found that this did not happen in the way it had been described. Instead, what it was found to have done was to target undecided voters who already had a clear tendency to vote for Trump and finally push them off the fence (especially because Republican voters are less likely to go and vote than Democrat voters). See: https://carasycaretas.org.ar/2020/11/05/quien-toma-tus-decisiones/

7 Strategy Lab, How Facebook Influences elections: The Great Hack Documentary.
Available at: https://strategylab.ca/how-facebook-influences-elections/

8 Giving people ownership of their **personal data** (2018). An example is the Decode project, which plans to make Barcelona a smart city but with a different logic whereby the rules of the game are not determined by the market. See: https://decodeproject.eu/

9 Parminder, Jeet Singh. 2019. Derechos en la sociedad de datos. Fundación Friedrich Ebert Regional, Montevideo, Uruguay, http://library.fes.de/pdf-files/bueros/uruguay/16201-20200529.pdf

10 Scasserra, Sofía and Sai, Leonardo Fabián. 2020. La cuestión de los Datos,
Plusvalía de vida, bienes comunes y Estados inteligentes. Fundación Friedrich Ebert Argentina.
http://www.fes.org.ar/public/LA%20CUESTI%C3%93N%20DE%20LOS%20DATOS.pdf

11 Ha-Joon Chang, *Kicking Away the Ladder–Development Strategy in Historical Perspective,* Anthem Press, London, 2002

12 World Trade Organization, Electronic Commerce (1998)
https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

13 James, Deborah. 2020. *Digital trade Rules, A disastrous new constitution for the global economy written by and for Big Tech.* Rosa Luxemburg Stiftung. https://www.rosalux.eu/en/article/1742.digital-trade-rules.html

14 The New York Times (2020) The big tech lobbying Europe.
Available at: https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html

15 Corporate Europe Observatory (2020) Big Tech brings out the big guns in fight for future of EU tech regulation.
Available at: https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation

16 Clauses included in other chapters of EU FTAs such as those on finance or telecommunications are not included in the analysis. Neither are domestic regulatory measures or market access clauses, which also affect the digital economy.

17 Compiled by the authors based on the text of the agreements mentioned. Where it says PARTIAL, this is because willingness to continue working on the agenda in the future is mentioned, but there are no explicit agreements on the issue.

18 The agreement can be read here: EU – CANADA (2018)
https://ec.europa.eu/trade/policy/in-focus/ceta/ceta-chapter-by-chapter/

19 The agreement can be read here: EU – SINGAPORE (2018)
https://trade.ec.europa.eu/doclib/press/index.cfm?id=961

20 The agreement can be read here: EU – VIETNAM (2018)
https://trade.ec.europa.eu/doclib/press/index.cfm?id=1437

21 The agreement can be read here: EU – MERCOSUR (2019)
https://trade.ec.europa.eu/doclib/press/index.cfm?id=2048

22 The agreement can be read here: EU – JAPAN (2017)
https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684

23 The agreement can be read here: EU – MEXICO (2018)
https://trade.ec.europa.eu/doclib/press/index.cfm?id=1833

24 World Trade Organization. 11th Ministerial Conference – Buenos Aires (2017). For information on how the exceptions have evolved, see the article by Sanya Reid Smith, Some preliminary implications of WTO source code proposal, available at: https://www.twn.my/MC11/briefings/BP4.pdf

25 European Commission/Cecilia Malmström/Trade for all. (2015)
https://trade.ec.europa.eu/doclib/docs/2015/october/tradoc_153846.pdf

26 General Data Protection Regulation. (2016) https://gdprinfo.eu/

27 European Commission (2019) DG TRADE Strategic Plan (2016 – 2019) https://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154919.pdf

28 Klaus Schwab. 2016. World Economic Forum, Fourth Industrial Revolution. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

29 European Commission. European Data Strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

30 Adam Satariano and Matina Stevis-Gridneff (2020) *Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators.* The New York Times https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html

31 Corporate Europe Observatory. (2020) *Big Tech brings out the big guns in fight for future of EU tech regulation.* https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation

32 The agreement can be read here: The texts proposed by the EU for a Deep and Comprehensive Free Trade Area (DCFTA) with Tunisia (2016) https://trade.ec.europa.eu/doclib/press/index.cfm?id=1490

33 The agreement can be read here: EU – CHILE (2021) Commission releases its proposals and reports about progress. http://trade.ec.europa.eu/doclib/press/index.cfm?id=1793&title=EU-Chile-trade-talks-Commission-releases-its-proposals-and-reports-about-progress

34 The agreement can be read here: EU-Indonesia (2018) EU provisions on *Cross-border data flows and protection of personal data and privacy* in the Digital Trade Title of EU trade agreements https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf

35 The agreement can be read here: EU-Australia (2018) Trade Agreement negotiations https://trade.ec.europa.eu/doclib/press/index.cfm?id=1865

36 EU-New Zealand. April 2021. The agreement can be read here: https://trade.ec.europa.eu/doclib/press/index.cfm?id=1867

37 On 2 October 2019, the EU launched negotiations with five partners in Eastern and Southern Africa (known as the ESA countries: Comoros, Madagascar, Mauritius, Seychelles and Zimbabwe) to deepen the existing Economic Partnership Agreement. The proposed agreement with these countries can be read here: https://trade.ec.europa.eu/doclib/docs/2021/january/tradoc_159393.pdf The title on digital trade starts on page 61.

38 The agreement can be read here: Joint Statement on electronic commerce (2019) WTO. https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf

39 TWN Info Service on WTO and Trade Issues (Dec 17/28) 2017. Third World Network. https://www.twn.my/title2/wto.info/2017/ti171228.htm

40 To see arguments of this sort, visit the UNCTAD web page on the E-Commerce Week https://unctad.org/meeting/ecommerce-week-2019-digitalization-development or the WTO Public Forum https://www.wto.org/english/forums_e/public_forum19_e/public_forum19_e.htm where there are various panels defending this stance.

41 OECD (2018) Bridging the digital divide. Include, upskill, innovate. http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf

42 Researchgate (2016) Gender Differences in Technology Usage–A Literature Review https://www.researchgate.net/publication/290475791_Gender_Differences_in_Technology_Usage-A_Literature_Review

43 Sofía Scasserra, 2016. E commerce, Future of labor and its impact on women. UNTREF. https://itforchange.net/draft/e-commercer-future-of-labor-and-gender-gap.pdf
UNCTAD (2021) Trade and Gender Linkages: An analysis of Least Developed Countries–Teaching Material on Trade and Gender: Module 4E (UNCTAD/DITC/2021/1).
Available at https://unctad.org/webflyer/trade-and-gender-linkages-analysis-least-developed-countries

44 APWLD (2017) 164 women's rights groups call on governments to reject the WTO declaration on women's economic empowerment. Available at: http://apwld.org/press-release-164-womens-rights-groups-call-on-governments-to-reject-the-wto-declaration-on-womens-economic-empowerment/

45 These arguments can be seen in various panels in the WTO Public Forum, for example. https://www.wto.org/english/forums_e/public_forum18_e/pf18programme_e.htm https://www.wto.org/english/forums_e/public_forum19_e/public_forum19_e.htm

46 https://unctad.org/system/files/non-official-document/eweek2018c01FED_en.pdf

47 Elaine Knutt,19/02/2021. WTO appoints Ngozi Okonjo-Iweala as new director general. Global Government Forum. https://www.globalgovernmentforum.com/wto-appoints-ngozi-okonjo-iweala-as-new-director-general/

48 Big Tech brings out the big guns in fight for future of EU tech regulation.12/2020. Corporate Europe Observatory. https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation

49 Huawei: UK government weighs up ban of Chinese firm's telecoms kit. July 2020. BBC https://www.bbc.com/news/technology-53306809

50 Free trade agreement that includes a large number of countries in Asia and Oceania.

51 Mauricio Claver Carone, 26/08/2020. Infobae. Candidato de Trump para el BID quiere limitar la influencia de China. https://www.infobae.com/america/agencias/2020/08/26/candidato-de-trump-para-el-bid-quiere-limitar-influencia-china/

52 Free trade agreement between the US and the EU that was signed but never approved.

53 Negotiations on them continue, but the neoliberal direction these rules are going to take has already been decided.

54 Based on Article 1 of the proposed digital economy agreement between the EU and Indonesia. Available at: https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

55 See: Australian Government, Department of Communication. Cloud Computing and Privacy Consumer Factsheet. Available at: https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf; Luiza Ch. Savage (2013), Trade Agreements, Privacy, and the Cloud, Available at: http://www.macleans.ca/uncategorized/trade-agreements-privacy-and-the-cloud/; ITI (2017) Data Localization Snapshot, Available at: https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

56 Wikipedia. General Data Protection Regulation. Available at: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

57 European Commission (2020), A European strategy for data. Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

58 Based on Article 1 of the proposed digital economy agreement between the EU and Indonesia. Available at: https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

59 WEF (2020) Where data is stored could impact privacy, commerce and even national security and here is why. Available at: https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/

60 Global 5G: Rise of a Transformational Technology. (2020). https://www.5gamericas.org/global-5g-rise-of-a-transformational-technology/

61 What Google does when a government requests your data. January 28, 2013. https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/

62 Colocation America (2020). The Future of Data Centers Renewable Energy. Colocation America. https://www.colocationamerica.com/blog/renewable-energy-data-centers

63 Technative (2020) Are Data Centres Helping The Economy? https://technative.io/how-data-centres-are-helping-the-economies/

64 Data Localization Snapshot. (2017). https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

65 Inland revenue. Tax Technical. Diverting personal services income by structuring revenue earning activities through a related entity such as a trading trust or a company: the circumstances when Inland Revenue will consider this arrangement is tax avoidance http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html

66 Wikipedia. Data haven. Available at: https://en.wikipedia.org/wiki/Data_haven

67 Statista. (2021) Revenue from big data and business analytics worldwide from 2015 to 2022. Available at: https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/

68 CEPAL (2016) La nueva revolución digital: de la Internet del consumo a la Internet de la producción. Available at: https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-Internet-consumo-la-Internet-la-produccion

69 Nathan Reiff (2021) How Visa Makes Money. Available at: https://www.investopedia.com/how-visa-makes-money-4799098

70 Based on Article X.9 of the proposed digital economy agreement between the EU and Indonesia. July 2017. Available at: https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf

71 Cody Cook, Rebecca Diamond, Jonathan V. Hall John A. List, and Paul Oyer. May 2020. The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers https://web.stanford.edu/~diamondr/UberPayGap.pdf

72 O'Neil, Cathy. 2016. Weapons of math destruction. Crown Books.

73 Data USA. Percentage of professionals in the IT sector IT by race or ethnicity. https://datausa.io/profile/soc/151251

74 The concept of open source refers to a type of software based on a model of open collaboration. It means that the source code is openly shared on the understanding that there are practical benefits of sharing the code (for example, when more people are studying a code and working to improve it or find vulnerabilities, the result is a better code, and therefore a better product). Open-source code differs from free software in that in the case of the latter the rationale for sharing the code is based on moral and philosophical arguments.

75 Closed-source software is the opposite of open source and refers to a source code that is not available to all users – in other words, it is not made public. This is frequently the case in companies whose IT system is seen as a valuable competitive resource. What they do is sell licences to use the system, without making it possible for any competitor to study the code and improve it. More information about the difference between the two types of code can be found in Guido Schryen (2009) Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. Available at: https://www.researchgate.net/publication/220891308_Security_of_Open_Source_and_Closed_Source_Software_An_Empirical_Comparison_of_Published_Vulnerabilities

76 For more information on this, the paper by Sanya Reid Smith (2017) is highly recommended. Available at: https://www.twn.my/MC11/briefings/BP4.pdf

77 Zeynep Tufekci, 2015. Volkswagen and the Era of Cheating Software. The New York Times. https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html

78 Based on Article X.3 of the proposed digital economy agreement between the EU and Indonesia. September 2017. Available at: https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf

79 Word Economic Forum. 5G Global Accelerator. https://www.weforum.org/projects/5g-global-accelerator

80 Rashmi Banga, *'Rising Product Digitalisation and Losing Trade Competitiveness',* United Nations Conference on Trade and Development.

81 Joseph Spanjers and Matthew Salomon, *'Illicit Financial Flows in Developing Countries Large and Persistent'*; Global Financial Integrity, Washington, DC, 2017. http://www.gfintegrity.org/report/illicit-financial-flows-to-and-from-developing-countries-2005-2014/

82 Brian O'Keefe and Marty Jones, 'Revenue Do-Si-Do: How Uber plays the tax shell game', Fortune Magazine, 22 October 2015, http://fortune.com/2015/10/22/uber-tax-shell/

83 Rashmi Banga, *'Rising Product Digitalisation and Losing Trade Competitiveness',* United Nations Conference on Trade and Development.

84 Based on an abbreviated version of Article 45 in the chapter on services in the EU-Mercosur agreement. Italics added. Available at: https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf

85 AirBNB Watch. Airbnb's Not So Sweet 16: Broken Neighborhoods. Available at: https://airbnbwatch.org/airbnbs-not-sweet-16-broken-neighborhoods/

86 Uber granted 18-month London license as judge overturns ban. CNBC (2020). https://www.cnbc.com/2020/09/28/uber-granted-temporary-london-license.html

87 GATT and GATS are the WTO agreements on the trade in goods and services, which establish the multilateral trade rules governing global trade.

88 *"Some of the implications of ecommerce proposals for government procurement"* by Sanya Reid Smith, Legal Advisor, Third World Network, 10 December 2017.

89 Based on an abbreviated version of Article 6 in the chapter on digital trade in the agreement between the EU and Mexico. April 2018. Italics added. Available at: https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf

90 Zetter, K. (2012). Rare legal fight takes on credit card company security standard and fines. Retrieved from https://www.wired.com/2012/01/pci-lawsuit/

91 Naureen S. Malik, "Cyberattack" Wake-Up Call "Puts Pipeline Industry in Hot Seat", Bloomberg (2018). Available at: https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat

92 Based on Article 49 in the chapter on services in the EU-Mercosur agreement. 28 June 2918. Available at: https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf

93 Jordan Graham, 20 April 2017 'Bose is accused of recording, selling audio information', Boston Herald.

94 Mike Isaac and Steve Lohr, (2017). *'Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data',* The New York Times.

95 Alex Hern, 14 March 2017 *'Vibrator maker ordered to pay out C$4m for tracking users' sexual activity',* The Guardian.

96 Issie Lapowsky, 17 March 2019. 'How Cambridge Analytica Sparked the Great Privacy Awakening', wired.com.

97 Cambridge Analytica in Latin America: What We Know So far. (2018). TeleSurHD. https://www.telesurenglish.net/analysis/Cambridge-Analytica-in-Latin-America-What-We-Know-So-far-20180322-0028.html

98 Based on Article 48 in the chapter on services in the EU-Mercosur agreement. 28 June 2019. Available at: https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf

99 Based on Article 2 of the chapter on cross-border data flows in the EU-Indonesia agreement. July 2018. Available at: https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

100 European Commission. (2016) Adequacy Decisions. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

101 Laufer, W.S. (2013) Social Accountability and Corporate Greenwashing. Journal of Business Ethics 43, 253–261 (2003) doi:10.1023/A:1022962719299 and Koehler, D. (2007) The Effectiveness of Voluntary Environmental Programs–A Policy at a Crossroads? Policy Studies Journal Vol 35, Issue 4

102 Based on an abbreviated version of Article X.10 in the chapter on digital trade in the EU-Indonesia agreement. Available at: https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf

103 Based on an abbreviated version of Articles 68, 69 and 70 in the chapter on the trade in services in the EU-Tunisia agreement. April 2016. Available at: https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154487.pdf

104 Denunciaron a Facebook por la venta de animales protegidos.18/10/2017. Diario Uno. https://www.diariouno.com.ar/mendoza/denunciaron-a-facebook-por-la-venta-de-animales-protegidos-10192017_H1fZQCIz0M

105 La ONU advierte del aumento de trata de mujeres y niñas a través de las redes sociales en el contexto de la pandemia (2020). Telemadrid. http://www.telemadrid.es/noticias/sociedad/ONU-advierte-sociales-contexto-pandemia-0-2286071375--20201112105748.html

106 Christina M. Ward. (2020). Pedophilia is Alive on Facebook Report These Pages Immediately! https://aninjusticemag.com/pedophilia-is-alive-on-facebook-report-these-pages-immediately-9ec2f3ea9296

107 David McCabe and Ana Swanson (2019). 'U.S. Using Trade Deals to Shield Tech Giants From Foreign Regulators', The New York Times.

108 Rodrigo, Chris (2020). Tech CEOs clash with lawmakers in contentious hearing. https://thehill.com/policy/technology/523268-tech-ceo-clash-with-lawmakers-in-contentious-hearing

109 Jaime Altozano (2020). Los algoritmos de YouTube censuran un vídeo paródico de Pantomima Full sobre los negacionistas del coronavirus. El diario.es https://www.eldiario.es/tecnologia/youtube-censura-video-parodico-pantomima-full-negacionistas-coronavirus_1_6263109.html

110 Based on an abbreviated version of Article 71 in the chapter on the trade in services in the EU-Tunisia agreement. (2016). Available at: https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154487.pdf

The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For more than 40 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org