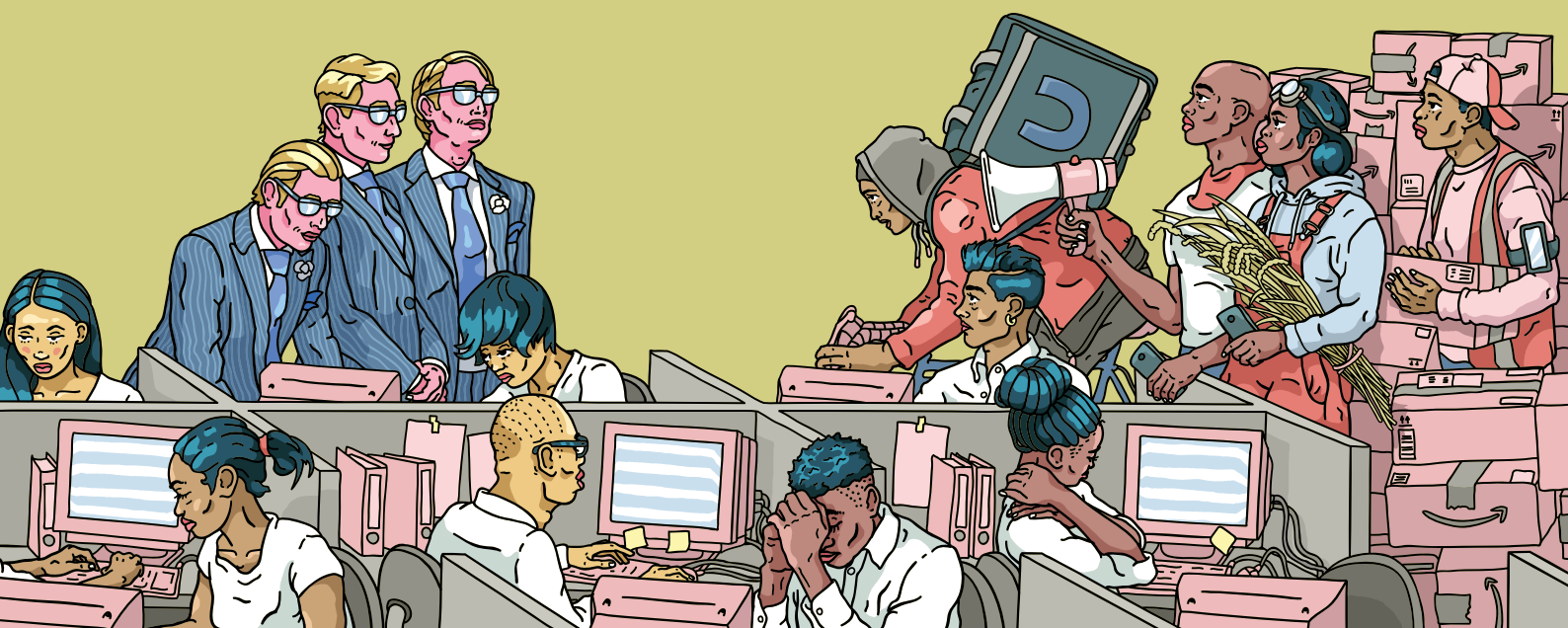
tni 50 years 1974 - 2024

WEEK 4

The digital trade agenda



1 Introduction

After World War II, the institutions that today make up the system that regulates the global economy began to be created. Among these institutions, one set out to regulate trade. Trade, it was said, brought peace. Avoiding protectionism and a new economic depression after the terrible recession of the 1930s seems key to building a new postwar world. At first glance, it seems logical: to trade more easily and quickly, standard norms and agreements on basic issues are needed to streamline transactions, and that was the initial intention of this new institution (or so it seemed).

Thus, in the post-war economy, the GATT (General Agreement on Tariffs and Trade) was born, which regulated border taxes. This agreement was born with a liberal idea of the economy: if there is more trade, we all benefit. Its design aimed for countries to progressively lower the taxes they charge for importing and exporting their goods. This agreement did not take into account that there are times when governments need to raise tariffs for strategic reasons, to defend local industries or due to shortages. The corporate and liberal idea took precedence over its creation.

The GATT did not remain a mere signed agreement; in 1994, it was transformed into an institution. This gave birth to the controversial World Trade Organization. This organization began to regulate much more than import and export tariffs to address whole swathes of the economy: trade in services, investment, intellectual property, domestic and customs regulations, and standards, among many others, mainly because the argument arose that there were many non tariff barriers to trade and a more comprehensive approach was needed. It did not take long for the rules approved and implemented to show their contradictions and cause harm to the countries of the Global South. In 1999, only 5 years after its creation, these injustices were so evident that the Seattle Round[1] negotiations were paralyzed as a result of popular demonstrations in the streets and 'developing' countries' disagreement. This led to the Doha Round in 2001, where developing countries were promised that no new issues would be negotiated until the inequities of the current system had been resolved.

But, already at that time, the growing importance of the digital economy was beginning to be seen. And just as the trade agenda was used to set neoliberal rules on issues outside the realm of trade, a strategy also emerged to make the Internet a place to do business, without state intervention, where corporations could take over something that seemed to be decentralized and in the power of all...

2 Architecture for digital liberalism

Since its creation by the US military, the Internet has always been an anarchic space. If one really wants to see the effects of economic liberalism, it is enough to see how a space that belonged to everyone and to no one was slowly but relentlessly transformed into a space dominated by monopolistic corporations. A place without rules only left us with greater concentration and total privatization of space.

States, at first, especially in low and middle income countries, did not seem to realize what was happening. Then, over the years, especially after the Cambridge Analytica scandal and the Myanmar genocide, state authorities began to question little by little whether they should not regulate, whether they should not tax, whether they should not question the technology, and whether they could not keep some of the Internet for interests other than those of corporations. Of course, this is quite different across different countries and different realities, but be it as it may, the international debate over the regulation of the internet and big tech companies has only appeared in the last couple of years.

There are two positions in this matter. We can say that states came too late to the stage and that corporations already have as much power as the States themselves, we can get discouraged and believe that the battle is lost. Or we can see what is really happening in governance and get to work in the fight to reclaim the Internet space.

The agenda containing the liberal rules of the game of the digital economy was first known as “e-commerce”. This name is not whimsical: it purported to show that it was only concerned with addressing buying and selling on the Internet. However, it’s actually seeking to deregulate the virtual space by and for corporations, limiting the regulatory capacity of States so that even if states eventually understand how to regulate, they will be unable to do so. It is worth pointing out that the internet has been, in the last couple of decades, a rule-free world, where the biggest and most aggressive companies won the territory until they dominated the market. What they intend to do by setting a deregulatory agenda within the WTO, is lock in deregulation once and for all, keeping in mind that states can and will try to regulate eventually. On the other hand, to set a deregulatory agenda makes it hard for small companies from the global south to enter the market, therefore kicking away the ladder to digital development among other countries. Corporations know that it is the right moment to set these rules and therefore are making big efforts in terms of lobbying to set new “e-commerce” rules into the WTO and other free trade agreements.

The e-commerce agenda has been negotiated at the WTO under the Joint Statement initiative (JSI) on E-commerce, but similar agreements with similar clauses have already been approved in numerous bilateral and regional free trade agreements. The e-commerce programme first started in the WTO in 1998, way before we had smartphones and social media. At that moment the biggest agenda being negotiated was the tax free data movement across borders, as we will see later. Recently the JSI started being negotiated and it is currently stuck, but some states (like the US) are pushing for it to come to an agreement. meanwhile, the text of the JSI is sneaking into "e commerce chapters" inside different free trade agreements,

It is important to understand that this agenda is illegal in the WTO for several reasons:

a. In theory, no new topics should be introduced until the Doha round is resolved.
b. A plurilateral agreement cannot be negotiated in the WTO, and the e-commerce program does not involve all member states, but only those that wish to participate.

Developing countries have been forced to join the negotiation with arguments such as "either you enter the negotiation or you look from outside". The truth is that this statement is false because there is very little that developing countries can propose and achieve in the negotiation. The articles are already drafted and what is being negotiated is really minor issues between China, the US and the EU. In essence the agenda is seeking to implement and consolidate a system for deregulation, turning the internet into a place of business and not of democracy, participation, and rights. It prevents a digitalization agenda, where public services are accessed freely, where data is generated for the public well-being, and where everyone benefits equally.

But what are these rules that consolidate corporate power and the power of the richest nations?

The big rules that corporations are trying to impose are in sum:

- Cross-border data transfer: Allowing companies to take private data, such as health data, out of the country in which it is sourced, and not allowing access to it ever again.
- Prohibition on data localization and processing: preventing developing countries develop their own data systems and excluding them from the value chain
- Non-disclosure of software and algorithm source-code
- tax free extraction of the biggest raw material of the digital economy: data.

among many others. We will analyze some of them now, so you get a sense of what is at stake in these types of negotiations.

3 What e-commerce agreements say and what they mean

Cross-border data transfer

What do e-commerce agreements say?

The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy.[2]

What does this imply?

Digital extractivism

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, which includes pre-paid medicine, private clinics, pharmaceutical industry, laboratories (Australian Government, 2014; ITI, 2017; Savage, 2013). The European Union has a law that protects the privacy of its citizens' data, known as GDPR.[3]

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 (European Commission, 2020). 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 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 data 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 anonymized data is vital for the design of future effective public policies.

4 Prohibition on data localization and processing

What do e-commerce agreements 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. making 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.

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 (Determann, 2020). 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 enables many outcomes. 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- Then, 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 (Rysavy Research, 2020). When 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 (Whittaker, 2013).
- It creates advanced technology subsystems within the economy. A data storage and processing center requires specialized staff to assemble and maintain it, the production of hardware and software to run it, fiber 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 centers 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 minimize the environmental impact (Colocation America, 2020).
- 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 center requires engineers, programmers, mathematicians, and a whole range of highly skilled workers (Kumar, 2020).

5 Non-disclosure of the source code of software and related algorithms

What do e-commerce agreements 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.

What does this imply?

Inequality, poverty, exclusion and unfair competition

To gain a broad understanding of this clause in free trade agreements, you need to remember what an algorithm is and how it works. We saw this in Unit 1 of this course.

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 and transform it into information. 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 tumor; an algorithm assigns orders to delivery drivers.

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 (Cook, Diamond, Hall, List & Oyer, 2020). 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. Biases are numerous and they have a huge impact on society.

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.

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 defense 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[4] are usually more reliable than closed-source software,[5] 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 the 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 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.[6]

6 Elimination of customs duties on digital products and/or electronic transmissions

What do e-commerce agreements 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.

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. In cities with driverless buses, the driver is likely to be an algorithm in a data center 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.

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 smartphones existed and before everything could be sold online.

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.

7 Prior authorization

What does it say?

1. The Parties shall endeavor 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.

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.

8 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.

What does this imply?

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

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.

9 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 send 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.

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 are detected 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.

There are many more clauses that were not included in this text. To further read about them and their implications we recommend to read:

https://www.tni.org/files/publication-downloads/digital-colonialism-report-tni_en.pdf

https://www.rosalux.eu/en/article/1742.digital-trade-rules.html

10 The new Global Digital Compact

In 2018 the Secretary General of the United Nations appointed a High Level Panel co-chaired by Jack Ma and Melinda French Gates to advise him. One cannot disagree with the semantic categories of the SG's report – from digital inclusion to human rights, it's all there. But the core diagnostic about what exactly ails our interconnected world unfortunately falls short. The solution simply misses the point.

The document calls for a Global Digital Compact (https://www.un.org/techenvoy/) to strengthen the governance of global digital commons and public goods.

However, it contains no recommendations for new legally binding intergovernmental treaties or rules to enhance the implementation of the international rule of law vis-à-vis emerging digital public goods. On the contrary, it argues that this does not require new institutions but rather multistakeholder cooperation. It seems unbelievable that with so many international institutions and with the growing importance of the digital arena, we do not have a system to regulate and control digital tools.

The report on which the Sec Gen's Roadmap is based, identifies a lack of trust and humility as the key problems preventing effective multi-stakeholder cooperation.

Multistakeholderism does not fail because of lack of humility or trust. It fails because, in a fundamentally unequal world, "the materially strongest nodes of the network will dominate the overall network. In any such network with no clear lines of responsibility, it is impossible to hold any actor accountable for any particular governance failure".

The unfortunate blind-spot in the SG's report is **as Anita Gurumurthy points out**, the extraordinary power of transnational digital corporations whose primary stake in digital cooperation is about ensuring the status quo.

If we are thinking about a digital governance that works for all, we need to counterbalance the power of corporations in the design of that governance. The GDC is right now being discussed and it has no clear outcome yet, but the multistakeholder approach seems to weigh the balance in the wrong direction.

In early 2023 a group of organizations (called the Global Digital Justice Forum) submitted a joint input for the GDC. The work of the group (individually and collectively) claims for a vision towards and practical action for:

a. democratizing the governance of digital technologies and promoting decentralized digital systems;
b. upholding the Internet as a global commons that can decentralize knowledge and power in our society and economy, enabling global exchange of information and knowledge, vibrant peer production cultures, sustainable local economies, free expression and association, and democratic deliberation and participation;
c. privileging a people-led, ecologically responsible, non-extractive, rights-enabling and gender-just vision of technology models that furthers a new international order rooted in development sovereignty;
d. calling for an end to corporate impunity; and
e. developing legal-policy frameworks for data, AI, and platforms grounded in human rights and economic justice on both transversal technological aspects and domain-specific/sectoral issues.

The members of the Global Digital Justice Forum consider the GDC as an important milestone that could (as the UN SG asserts in his Report to the Commission on Science, Technology and Development) become an opportunity for Governments and other stakeholders to revitalize international cooperation in the light of the dramatic changes that have taken place in digital technology. You can read the complete submission **here**.

11 Why is digital governance important?

Digitality has become the new way in which the economy is shaped. We think about markets, about buying and selling, about organizing the economy, and we think about digital tools.

In some sense, we could point out that the planification of our global economy is made these days by big tech companies: they are the ones sending tools to medium and small enterprises and transforming data into information that is going to lead to decisions on how, when, and where we produce goods and services. Digital tools are everything in today's economy. Almost any sector of the economy is organized, administered, or controlled by digital tools, most of which are not completely made at the national level, especially in low and middle income countries. These digital tools are not only leading the economy, but also a big resource of power and money in the economy: to be able to produce digital tools is not only sovereignty but also being able to produce in a high quality industry with relatively good paid jobs. Therefore, limiting the competition and allowing the monopolization of the market and the information is a new way to kick the ladder to digital industrialization in the global south.

We live in a digital world. More and more not only the economy, but our basic rights have a digital sphere: access to education, to health, to culture, to information, are all spheres of our lives that happen on the web as well as offline. Therefore, we need rules and regulations in order to limit what the market (and corporations) can and cannot do on the internet. Economic logic cannot prevail in a digital world where basic human rights are exercised. We need a global governance that is based on people and to access these rights online. The trade agenda certainly does not go into that direction and the GDC falls short into its architecture.

REFERENCES

Australian Government (2014), Cloud Computing and Privacy Consumer Factsheet. Department of Communication. Available at: https://www.infrastructure.gov.au/sites/default/files/2014-112101-CLOUD-Consumer-factsheet.pdf

Cook, C., Diamond, R., Hall, J., List, J., & Oyer, P. (2020). The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers. *The Review of Economic Studies*, *88*(5), 2210-2238. Available at: https://web.stanford.edu/~diamondr/UberPayGap.pdf

Colocation America (2020, January 30). The Future of Data Centers Renewable Energy. Colocation America. https://www.colocationamerica.com/blog/renewable-energy-data-centers

Determann, L. (2020, June 9), Where data is stored could impact privacy, commerce and even national security and here is why. *World Economic Forum.* Available at: https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/

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

ITI (2017), Data Localization Snapshot. Available at: https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

Kumar, S. (2020, August 4), Are Data Centres Helping The Economy? *Technative.* Available at: https://technative.io/how-data-centres-are-helping-the-economies/

O'Neill, C. (2016). Weapons of math destruction. *How Big Data Increases Inequality and Threatens Democracy*, *10*, 3002861.

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

Savage, L. (2013, June 17), Trade Agreements, Privacy, and the Cloud. *Maclean's.* Available at: http://www.macleans.ca/uncategorized/trade-agreements-privacy-and-the-cloud/

Schryen,G. (2009). Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. *AMCIS 2009 Proceedings*, 38. Available at: https://www.researchgate.net/publication/220891308_Security_of_Open_Source_and_Closed_Source_Software_An_Empirical_Comparison_of_Published_Vulnerabilities

Whittaker, Z. (2013, January 28). What Google does when a government requests your data. *ZDNet*. Available at: https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/

NOTES

1 The Ministerial Rounds (as they are popularly known) are the decision-making body of the WTO and should meet every 2 years on a regular basis.

2 All the transcripts of the articles of the e-commerce agreement were taken from the proposed digital economy agreement between the EU and Indonesia. Available at: https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

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

4 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.

5 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

6 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

The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For nearly 50 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org

CO-SPONSORED BY:

SOMO

IT for Change

statewatch

DigitalCapitalismCourse.tni.org