TRADE & INVESTMENT POLICY BRIEFING | November 2021

Indonesia’s digital economy commitments in EU and RCEP trade agreements

An analysis

Sofia Scasserra

Indonesia for Global Justice

tni
transnationalinstitute

In recent years, Free Trade Agreements (FTAs) have started to include rules for the digital economy as a result of pressure from Big Tech. These trade measures are potentially damaging to a country's possibilities of digital industrialisation, permanently locking in advantages for the richest nations. This summary analyses the most important points being negotiated by Indonesia with the European Union and RCEP.

CONTEXT

Negotiation of the free trade agreement between Indonesia and the EU began in 2016. Many of EU's positions were typical of various free trade agreements, but noticeably it also included new requests related to digital trade. The new demands suggest an EU strategy to achieve a level of digital dominance that could allow the region to think of itself as a player in the digital economy, where it currently lags far behind the US and China. It is already falling behind in terms of providing infrastructure for 5G. However, the battle for the digital services to be provided by the new network may still put the continent in a privileged position.

The EU is keen to insert itself into the Global Value Chains in an intelligent way. Strategically, it is seeking to accumulate data globally, which will allow the development of new services provided by European manufacturing companies. This implies a strategy of indiscriminate, colonialist digital extractivism that has up to now been carried out by the mainly US big technology companies, but in which European companies are now jostling for their own part of the pie.

But rather than search engines or stores, European companies are seeking to build 'smart' versions of their existing manufactured products. For example, an intelligent refrigerator wouldn't just keep food cold, It would also be capable of suggesting purchases and promotions in the local neighbourhood. All these services incorporated into industrial manufacturing are only possible if there is sufficient data storage and processing. To develop the Internet of Things in manufacturing, companies need a big amount of data (big data) which requires extracting the data, localising it and processing it in the European Union, keeping control of all the raw materials and the algorithms to process it.

The European Data Strategy[1] is thus a strategy to dominate digital capitalism through developing cybernetic value chains based on digital extractivism from the global South to the global North. This situation has also been strongly shaped by the strong lobbying efforts[2] of North American technology companies in the region, who have sought not only to construct a liberal model in the digital economy in trade relations, but also within the EU, seeking to minimise regulations that limit their extractive capacity in the European market[3.]

Indonesia has been negotiating these Free Trade Agreements for a long time now, without analysing the cost in terms of industrialization. The measures will put handcuffs on the state capacity to regulate and have their own data strategy. It seems like Indonesia is ready to be a provider of data to other countries wich will develop technologies and sell them back to the Indonesian people. It appears that the Indonesian state is content give up the possibility of digital industrializstion, transforming the country once and for all into a mere producer of data and a consumer of technologies designed and produced abroad.

These type of clauses are also present in RCEP, an FTA agreed and signed by various Asian and Pacific countries (Australia, Brunei, Cambodia, China, Indonesia, Japan, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, South Korea, Thailand, and Vietnam).This agreement is seeking to construct a new comercial bloc in Asia with China as the main leader, imposing norms that will expand its market. This is especially the case in terms of the digital economy given China's dominance in this sector. This agreement will prevent countries from adopting the same measures that the Chinese goverment implemented in order to become a leader in the digital market.

WHAT ARE THEY NEGOTIATING?

Europe's shift to focus on digital economy has taken a number of years, but by the time of its negotiation with Indonesia, the digital agenda had been put at the heart of its proposals. Cross border data flows were established as core articles.

RCEP, by contrast had this agenda present from its genesis. The Asian technological giants knew how to play the game of the predictive algorithms industry and China has supported them through a digital trade agenda that leads to data control supremacy in the region.

The following table summarizes the main commitments that Indonesia is in the process of assuming once the agreements with the EU and the RCEP finish and enter into force. Its good to clarify that for the purpose of this study, we have included only the provisions in the e-commerce chapters of both agreements. Other chapters might have provisions affecting the digital economy.

Measure	EU[4]	RCEP[5]
Cross-border data flows	YES	YES
Prohibition of data localisation	YES	YES
Prohibition of data processing in local country	YES	YES
Non-disclosure of software source code and related algorithms	YES	NO
Elimination of customs duties on digital products and/or electronic transmissions	YES	YES
Prior authorization	YES	NO
Non-discrimination against digital products	YES	PARTIAL
Electronic authentication and electronic signatures	YES	YES
Online consumer protection	PARTIAL	YES
Personal information protection	PARTIAL	YES
Measures against unsolicited commercial electronic communications	YES	YES
electronic public procurement	YES	NO

The first five provisions are the most far-reaching, with serious compromises that may result in permanent consequences for Indonesia both in terms of digital industrialisation capacity and in terms of social impact.

Provisions with most concerning consequences

To understand the real consequences that these provisions migth have on Indonesia, this briefing explains each proposal, its implications and of how it has or can impact on countries' economies and daily lives.

CROSS BORDER DATA FLOWS

What does it say?

The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy[6].

What does it imply?

This clause basically consists of digital extractivism. It implies that any company that starts operations in the territory with which it signed the agreement, can extract data from local consumers and citizens and take it to another territory without any restrictions. Thus, data, the raw material of artificial intelligence, and other technologies of the new industrial revolution, can cross borders and the state loses access to it. This is crucial to understand: once data crosses the border, access or repatriation cannot be demanded because the country loses jurisdiction over it. It is the equivalent of any physical asset we know of. Let's say a work of art or a precious mineral: once it crosses the border, the country is going to have a very difficult time getting that asset back into the territory, if it is ever possible.

Example

One of the central concerns regarding the possible consequences of approving the cross-border flow (or cross-border transfer) of data is the impact on the privacy of citizens, especially with regard to sensitive data, such as health data. In this regard, and taking into account the reality of the sale and purchase of data banks in the healthcare industry, countries such as Australia, among others, have strict privacy laws. In the case of the Australian government, Australian privacy law is more difficult to enforce if the provider of the data storage servers is based overseas. It is for this reason that Australia's electronic health records system has a requirement that the data remain and be processed in Australia. If an indiscriminate cross-border transfer of data were to be approved, Australia would not be able to establish the necessary protection for the privacy of its citizens' health data. This is also due to concerns about how big data can be used, especially in that area, which is one of the industries with the highest turnover (prepaid medicine, private clinics, pharmaceutical industry, laboratories)[7].

In terms of economic development, this data mining represents a vital raw material for the development of artificial intelligence, which leaves the territory and never re-enters. But also, it is also relevant information when designing public policy. Let's think for a moment how UBER data would be useful to develop an urban planning policy in the transportation system, or Google Classroom data during the Covid-19 pandemic for the Ministry of Education of any country. These examples try to show the importance of keeping the liberty to regulate over the movements of data across borders.

PROHIBITION OF DATA LOCALIZATION AND PROCESSING

What does it say?

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

a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;

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

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

d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory[8].

What does it imply?

Data as a raw material has several instances in its value chain. The movement of data across the border is the export of that raw material. But the value chain also has as fundamental components the processing and hosting of the data. These can occur independently of the export of the data. If we can briefly summarize this clause, we would say that it is digital colonialism and economic dependence. A country could include in its public procurement systems, when contracting digital suppliers, contractual clauses that request that these data remain in the country and that the State be given access to them in order to design public policies or, in the future, its own systems that can replace the supplier and achieve economic independence and contribute to digital industrialization. It could also pass a law containing minimum requirements for any company investing in the territory. With this clause in free trade agreements, such capacity would be limited. This is currently used by some countries and strongly resisted by the hegemonic lobby groups[9]. They argue that localization requirements allow abuse in the access of States to data. Although States migth want to protect industry and SMEs in the short term by not generating competition with foreign countries, companies argue that is detrimental to the economy: in other words, the localization of data in the territory does not favor the interests of transnational companies and makes it more difficult for them to compete against local companies.

The truth is that data localization is a strategic issue in the current and future economy, since having data servers nearby allows several things. For example:

Having faster and more effective information systems, otherwise triangulation occurs. A citizen uses a service and requests a search on the web, that request must "travel" to the server where the data is located, the request must be processed, and must return with the result. This takes a few miliseconds and is almost imperceptible to the population, but, with the advent of 5G, this will be of vital importance[10]. Indeed, in order to drive a smart car or perform remote surgery, it is necessary that this delay does not exist because it can cost human lives.

The fact that the data remains under the jurisdiction of the country that produces it also makes it possible to eventually request access to it for health or national security reasons, among others. It grants sovereignty over the data, allowing this strategic input to remain within the confines of a country and those who produced it. Today, if a government needs data from, for example, Google, it must request permission from the U.S. State Department, which in turn requests it from Google and finally shares it[11].

It generates high-tech economic subsystems, since a data storage and processing center requires specialized personnel to assemble and maintain it, hardware and software production, fiber optic networks to reach it, and, in many cases, even renewable energies, since many companies began to invest in autonomous energy systems for their data centers due to the risk of energy loss in the event of a failure in the national energy system and the cost savings it can bring, in addition to the environmental impact[12].

The processing, on the other hand, is generally done at the place where the data is stored to avoid double triangulation, which slows down the final delivery of the product. This point is also key, because that is where the greatest profit of the digital capitalist economy is generated. That processing is nothing more nor less than the algorithmic systems of data processing in real time and where there is the greatest amount of human labor of very high technological productivity. A data processing center requires engineers, programmers, mathematicians, and all kinds of highly skilled workers[13].

Example

One of the central reasons for maintaining the localization of data storage and processing is for security reasons, especially in matters that could affect a country's national security. This is the main reason the United States has a requirement that all cloud computing service providers storing Department of Defense data must be within its borders[14]. On the other hand, another reason to maintain localization is to have the ability to enforce the country's laws and avoid legal disputes being resolved in international or foreign courts. In the case of New Zealand, its government requires that tax records that are stored "in the cloud" be stored on servers located in New Zealand and failure to do so is an offense punishable by a fine. Cloud backups are enabled, as long as the primary business records are stored in New Zealand[15]. If this regulation is approved by the World Trade Organization, we could also see "data havens"[16] emulating the already known tax havens: places where transnational companies can host their data without having to respect security or data protection regulations or limit their processing, in order to obtain the maximum possible profit. These havens already exist, but if the regulations were to be implemented globally, it would be even more difficult for governments to combat them.

In addition, revenues from data processing and storage are growing globally[17]. Not only at the country level, but also within the companies themselves. At Visa, for example, 38% of revenues come from data processing[18]. In terms of regions, revenue from storing data in a country is growing by leaps and bounds, and of the total revenue from this service, 59.6% is from the US, 20% from Western Europe, 10% from Asia-Pacific and the rest is split between Africa, Latin America and Eastern Europe[19]. Clearly the business of storing data in the public cloud is concentrated in specific regions with a strong strategy of digital extractivism.

NON-DISCLOSURE OF SOFTWARE SOURCE CODE 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[20].

What does it imply?

Inequality, poverty, exclusion and unfair competition. To comprehensively understand this clause in free trade agreements, there are several concepts that we need to explain beforehand. On the one hand, what is an algorithm? In the digital economy everything is handled with them and it is what really processes the huge amount of data we generate on a daily basis. Algorithms are instructions, mathematical equations, that process information and return a result, be it a maximization, an ordering, a decision or a menu of options, among other things. When we do an internet search, an algorithm decides which results we will see first; when we enter Netflix, an algorithm decides which movies to show us; an algorithm processes medical images and indicates what is the probability that a certain spot is a tumor; an algorithm assigns orders to app workers when they go through the streets delivering orders.

This is what is known as Machine Learning and Deep Learning, two types of technologies within the field of Artificial Intelligence, and it is already widely documented that it has some difficult drawbacks. The concept of algorithmic bias is key here. Algorithms have very significant manufacturing biases that while they can be minimized, they are unlikely to be completely eliminated. To begin with, algorithms are fed with data, but that data is arbitrarily categorized and separated. From the binary sexual category to the choice of fruit and vegetable possibilities, the categories that are chosen for data entry can be biased and leave entire groups of data unrecorded and thus disregarded by an algorithm. In turn, the data are loaded with histories of violence and discrimination. It has been studied that female UBER drivers in the US earn 7% less[21] than their male counterparts, not because they drive worse or are worse hosts when it comes to taking a passenger, but because the population tends to rate them more negatively than men due to cultural aspects. Finally, there is a programming bias that is surely the most important. Deciding what is important and what is not important to an algorithm is ultimately a human decision. Cathy O'Neil has a very illuminating example in this regard[22]. She argues that she has an algorithm in her head that decides every night what to cook for dinner. The variables she has are nutritional assessment, items she has in the fridge, desire and time to cook, what she ate at noon, family tastes, etc. Her head processes that and decides what to cook that specific day. What would happen if her child took control of the algorithm? Surely nutrition would take a back seat and tastes would be predominant, resulting in french fries over fish. The biases are many and have enormous impacts on societies. If we add to that the fact that most of the algorithms we use on a daily basis are programmed in developed countries by white heterosexual men of a certain socioeconomic and educational level, we run the risk that minorities, dissidents and women are never taken into account. In fact, there are only 22% of women programmers worldwide. In the USA, the largest economy in the industry, 67.7% of programmers are white, 19.5% are Asian and less than 13% are black and other ethnicities.

Latinos are not even counted in the statistics[23].

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 and the source code is the instruction or how the order is intended to be developed. To use a legal example, the algorithm is the law, the source code would be the regulation.

In some countries, such as Argentina, the software (source code and executable) is protected under the Intellectual Property Law, within the framework of copyright. In these cases, despite the existence of such protection to sanction illegal copies, for example, access to read the code is not prevented. This prohibition could occur if the code or algorithm were protected by industrial secrecy, as some companies do. On the other hand, in other countries, such as the United States or Canada, software is protected under the patent system, which are titles that recognize the exclusive right to exploit functionalities, algorithms, representations and other actions that can be carried out with a computer for 20 years. In the case of patents, in order to grant that exclusivity, the code is also made public and no one else can use that code for the duration of the patent.

If I don't have access, I can't audit it to know what problems it is having in case something bad happens. The clause usually includes exceptions such as in the case of defense and national security or if there is suspicion that the algorithm is contrary to the country's competition laws. The truth is that it is difficult to build a case that demonstrates the need to audit the algorithm and that the exceptions do not take into account problems in the general population, such as the case of discrimination against workers or in facial recognition systems, to name a few.

On the other hand, it should also be clarified that even when the source code can be audited, it is almost never simple to find the error or problem that has arisen. Algorithms, in many cases through Machine Learning, are self-written and end up being unreadable for the programmers themselves. It should also be noted that on average, open source programs[24] are more reliable than closed source ones[25], so they bring more social benefits for the reasons described above.

In conclusion, it is a very complex problem to solve that humanity is just beginning to face and that can have multiple impacts on our societies, generating future discrimination, environmental problems, attacks on democracy and economic destabilization, among others. It does not seem to be, at first sight, a good measure to limit state capacity in the face of a problem that we are just beginning to learn about and that we do not yet know how to solve. The non disclousure of algorithms has been so problematic trougthout the years that even in free trade agreements, countries started to add more and more exceptions[26].

Example

Access to the source code may be requested for legal cases, for example for cases of intellectual property infringement of a software, accuracy in diagnostics and results (for example, the system of a breathalyzer in a case of a suspected drunk driver who wanted to check the accuracy of the system). Also, to know if the system generates or reproduces discrimination in certain populations, it may be necessary to access the code to study it and thus reduce vulnerabilities to hacking (for example, in electronic voting systems or systems used in sensitive areas such as health, security and public administration, critical infrastructure -such as nuclear power plants-, among others).

One of the reasons that governments may have for requiring access to the source code may be to verify that a particular regulation is being complied with. An example of this is the Volkswagen emissions scandal, when the car company used the software to pass the emissions test although, in reality, it was polluting up to 40 times more than the legal limit when driving[27].

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[28].

What does it imply?

This provition implies the hollowing out and defunding of the State. If we saw anything during the Covid-19 pandemic, it is that many of the things we thought would never be possible to digitize, they actually are. Education and telemedicine were the big changes, but others that were timidly gaining market share accelerated, such as online meetings and webinars, to name a few. The truth is that as technology advances, more and more of the economy will be delivered over the Internet. In fact, the 5G project plans to create smart cities, factories and homes, with machinery and appliances that are operated remotely from other countries[29]. Cities where buses have no drivers. The driver is probably in a data center in some remote territory and is an algorithm. All this will be possible. At the same time, with 3D printers, designs are marketed through the web that can be printed directly in the country that acquires the design. This opens up a whole new world of digital service exports, displacing manufacturing exports.

In this sense, prohibiting customs duties on electronic transmissions means not being able to charge taxes at the border for any of these services provided from abroad. It is a defunding of the State in the future.

While it is true that the clause does not prevent the collection of internal taxes (such as value added tax, for example), it does prevent the collection of customs taxes, which shows that the intention is not to grant lower prices to consumers, but that the objective is quite different. When the taxes are customs duties, it is the State that collects them directly upon entry into the territory and indirectly gives national products a differentiated treatment, since they do not have to pay them. It lowers the price of domestically produced goods compared to those produced outside the territory. On the other hand, internal taxes are charged by the companies directly to the user and it is the same company that is in charge of transferring the money to the State. This has several positive effects for transnational companies. Firstly, only a company with a digital infrastructure large enough to differentiate the taxes of each country in which it operates will be able to gain market share. Smaller competitors will find it difficult to sustain such a structure and will be more prone to make mistakes and thus lose the competition. Secondly, it gives them possession of extra foreign currency that they can delay in payment, and may produce extra interest with the management of those funds. Thirdly and finally, national treatment rules mean that if multinationals are charged an internal tax, that tax must also be applied to their local competitors. Economies of scale play a fundamental role where it is much more likely that national companies will not be able to compete at the cheap prices that multinationals usually have and will end up losing market share.

In an increasingly digital and globalized economy, not being able to collect customs duties on electronic transmissions is taking away the State's main source of financing and its capacity for national and sovereign digital industrialization, losing national technology companies to international competition.

Although this rule is being negotiated in Free Trade Agreements (FTA), it has already existed in the WTO for years through the Moratorium on Customs Duties on Electronic Transmissions (MCDET). It was agreed multilaterally in 1998, long before the digital revolution, smartphones and social networks modified the way we communicate and inform ourselves.

MCDET basically replicates the clause on non-payment of taxes on electronic transmissions in free trade agreements, but at the multilateral level, preventing developing and underdeveloped countries, net importers of digital services, from charging customs duties on them since 1998. This moratorium has been renewed every year since then and has never been reversed, generating a real fiscal loss for the global south.

The inclusion of this clause in free trade agreements is intended to ensure that if the moratorium is not renewed, the commitment will continue to be sustained through the diversity of existing FTAs.

Example

Digital liberalization will likely facilitate more imports of digitally-intensive products and services into developing countries, rather than exports from them. Proponents cloak their proposals in the Trojan horse of being necessary to "unleash development through the power of MSMEs (Micro, Small and Medium Enterprises) using e-commerce". But to trade, countries must generate and increase the value captured from production. If digital trade expands without first improving productive capacities in developing countries, as well as bridging the digital divide through improvements in physical infrastructure and interconnectivity and the adoption of enforceable standards for privacy, data protection and economic data rights, developing countries will simply open their economies further to foreign imports[30].

Global Financial Integrity identified transnational corporations that, in 2014, drained between $620 and $970 billion from developing countries, mainly through commercial fraud[31]. A concrete example is Uber that uses subsidiaries based in Ireland and the Netherlands to register the vast majority of its profits, accrued to its intellectual property, in the tax haven of Bermuda, leaving countries (from Kenya to the United States) where profits are generated, without proper tax rights[32]. The WTO protects them from paying taxes at the border, and they also use subsidiaries in tax havens to evade local taxes.

A paper prepared by the UNCTAD conducted a simulation exercise showing that if a permanent moratorium of zero tariffs on electronic products and transmissions is applied, there will be an additional increase in imports of these products to developing countries, while imports to developed countries will not be affected. In many cases, not all imports in this category are electronic transmissions, for example, in the case of music CDs there are still some imports that are not electronic transfers. As the digitization of products increases, more of these products will fall into the electronic transfer category. The increase in imports of these types of products, which are currently in this category, will be highest in absolute terms for China, followed by India, Russia and Brazil[33].

CONCLUSIONS

The emerging digital agenda that is evident in free trade agreements such as the one with EU and Indonesia or RCEP is largely being imposed on low and middle-income countries. Many countries do not necessarily forsee the consequences of the variety of commitments they are assuming by signing these agreements.

The message powerful countries such as EU and China deploy is that "Either you are sitting at the table negotiating or you just staring at the menú", giving a false sense that if countries get involved in the negotiations they are better off than just dropping out if them.

The truth is that most of the clauses are designed by corporations, looking for new profitable ways to extract digital raw material from low and middle income countries in order to expand profits and corporate control.

Low-income countries of course are limited in their capacity to develop a digital industrialisation strategy and to be able develop companies that are able to compete against these corporations. Nonetheless, new technologies can be designed within their borders based on a logic of data as a public good[34], focusing on social objectives and digital sovereignty. It is wise therefore that countries guard their policy space - and not embrace trade measures that restrict this - so they can develop digital tools that serve public services. Smart cities or indeed any social sectors which can be improved with technological tools will be better off without a profit logic. A just sustainable development requires developing technologies with social objectives, looking to embrace inclusion, equality, and development for all, not just a few.

A first step towards these objectives requires rejection of these digital trade measures.

NOTES

1 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

2 https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html

3 https://corporateeurope.org/en/2020/12/big-tech-brings-out-big-guns-fight-future-eu-tech-regulation

4 It was used only the Indonesia- EU digital trade chapter available at https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

5 It was used only the RCEP e commerce chapter. Available at https://www.dfat.gov.au/sites/default/files/rcep-chapter-12.pdf

6 Article 1 of the proposed EU-Indonesia digital economy agreement was used as a model. Available at https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

7 https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

http://www.macleans.ca/uncategorized/trade-agreements-privacy-and-the-cloud/ https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

8 Article 1 of the proposed EU-Indonesia digital economy agreement was used as a model. Available at https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

9 https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/

10 https://www.5gamericas.org/global-5g-rise-of-a-transformational-technology/

11 https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/

12 https://www.colocationamerica.com/blog/renewable-energy-data-centers

13 https://technative.io/how-data-centres-are-helping-the-economies/

14 https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

15 http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alert-ra1002.html

16 https://en.wikipedia.org/wiki/Data_haven

17 https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/

18 https://www.investopedia.com/how-visa-makes-money-4799098

19 https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-internet-consumo-la-internet-la-produccion

20 Article X.9 of the proposed EU-Indonesia digital economy agreement was used as a model. Available at https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf

21 https://web.stanford.edu/~diamondr/UberPayGap.pdf

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

23 https://datausa.io/profile/soc/151251

24 The concept of open source refers to a type of software that is based on a model of open collaboration, i.e. the source code is shared openly because it is understood that there are practical benefits to sharing the code (for example, more people studying a code and working on improving it or finding vulnerabilities, the result is a better code, therefore, a better product). Open source differs from free software in that the latter understands the logic of code sharing from moral and philosophical issues.

25 Closed source code is so called as opposed to open source code and refers to source code that is not available to any user, i.e. it is not made public. This is common in development companies that have as a value and competitive resource a computer system and what they do is to sell licenses to use that system, without enabling the possibility that any competitor can study the code and improve it. You can read more about the difference between both types of code here: https://www.researchgate.net/publication/220891308_Security_of_Open_Source_and_Closed_Source_Software_An_Empirical_Comparison_of_Published_Vulnerabilities

26 For more information on this, it is highly recomended t oread a paper done by Sanya Reid Smith available at https://www.twn.my/MC11/briefings/BP4.pdf

27 https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html

28 Article X.3 of the proposed EU-Indonesia digital economy agreement was used as a model. Available at https://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156106.pdf

29 https://www.weforum.org/projects/5g-global-accelerator

30 Rashmi Banga, 'Rising Product Digitalisation and Losing Trade Competitiveness', United Nations Conference on Trade and Development, June 2017. Available at https://unctad.org/system/files/official-document/gdsecidc2017d3_en.pdf

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

32 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/.

33 Rashmi Banga, 'Rising Product Digitalisation and Losing Trade Competitiveness', United Nations Conference on Trade and Development, June 2017. Available at https://unctad.org/system/files/official-document/gdsecidc2017d3_en.pdf

34 https://towardsdatascience.com/data-for-public-good-1414cbc99335

AUTHOR: Sofia Scasserra

COPYEDITOR: Nick Buxton

DESIGN: Evan Clayburg

Co-published by Transnational Institute and Indonesia for Global Justice

November 2021

transnationalinstitute

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

Indonesia for Global Justice

Indonesia for Global Justice's vision is “A Global Justice Order through Social Movements”. The mission of IGJ is “Changes toward a just trade system through developing critical awareness and empowering strategic groups of civil society”.

www.igj.or.id

TNI’s **Trade & Investment** project opposes the European Union’s corporate-driven trade and investment policies by providing well-researched analysis on its social and ecological impacts, supporting the development of popular campaigns and proposing alternative policies that prioritise people’s rights over corporate profits.

Sign up to receive receive regular updates from this project and TNI at www.tni.org/subscribe