Journal of Law, Market & Innovation

ISSUE 1/2023

Journal of Law, Market & Innovation

1/2023

Editors: Riccardo de Caria, Lorenza Mola, Cristina Poncibò

Journal of Law, Market & Innovation
Vol. 2 - Issue 1 - 2023
ISSN 2785-7867
Journal of Law, Market & Innovation

TABLE OF CONTENTS

Riccardo de Caria – Lorenza Mola - Cristina Poncibò

FOREWORD TO ISSUE 1/2023

In its first issue of every year, the JLMI hosts a section focused on international and comparative approaches to trade law, with the goal of offering to the readers challenging ideas, critical insights, and new perspectives. Such section is the result of a collaboration with the Turin School of Developments 'Master of Laws in International Trade Law, a post-graduate program jointly run by the Law Department of the University of Turin and the International Training Centre of the ILO in partnership with IUSE, UNCITRAL and UNIDROIT. This year's trade law section is devoted to 'Economic Sanctions and Innovation'. It focuses on the impact of technological innovation on governments 'economic sanctions against other countries and/or specific individuals. The section consists of the Innovation Letter by Professor Antonino Alì and of two articles. Two perspectives especially come into relevance: first, the role of innovation and technology in the design and enactment of sanction regimes; second, the way sanctions target, concern or involve innovation and technology.

This issue also features articles on: anti-money laundering laws; blockchain in monitoring the sanctioning regimes; "Big Tech" Responsible Business Conduct; on the question whether impeding competition is anticompetitive; on the revitalisation of the Essential Facilities Doctrine in EU Competition law; and on Sanctions, Open Source Software, and Opposing Trends in Sovereignty.

R.d.C. - L.M. - C.P.

*Antonino Alì**

INNOVATION LETTER

THE IMPACT OF INNOVATION AND TECHNOLOGY ON RESTRICTIVE MEASURES TARGETING THE RUSSIAN FEDERATION

Abstract
Since 2014, several countries imposed economic sanctions on Russia, including restrictions on technology exports to Russia's energy and defence sectors. However, these sanctions were not effective due to their vagueness and loopholes. In 2022-2023, to further restrict trade with Russia, new export controls and restrictions on dual-use goods and technology were introduced in the 9th and 10th packages of EU sanctions. The ban on the export of goods and technology relating to the aviation and space industry was expanded, and new items were included in the list of restricted items that could potentially enhance Russia's defence and security sector. Technology can play a crucial role in enhancing the effectiveness and efficiency of restrictive measures, as well as creating new ways for sanctions to be circumvented. However, technology can also be used to improve intelligence-sharing and data analysis related to suspected violations of sanctions, thereby enabling authorities to better identify and target violators.

JEL CLASSIFICATION: K33

SUMMARY

1 Autonomous coordinated sanctions against the Russian federation

Due to the destabilisation and invasion of Ukraine, economic and financial sanctions have been imposed on the Russian Federation, reflecting some of the most extensive and coordinated actions ever undertaken against a State of its prominence. The Russian Federation, a powerful military nation with nuclear capabilities, is characterised by one

* Associate Professor of International Law at the Faculty of Law and at the School of International Studies of the University of Trento.

of the world's largest economies by GDP and serves as a significant exporter of raw materials, energy, and agricultural products. Since 2014, restrictive measures against Russia have been gradually implemented as a response to the country's violation of Ukraine's sovereignty and the annexation of Crimea. The legal framework of the sanctions so introduced remained largely unaltered until 2021. Although there have been some changes to the framework of the sanctions over the years, such as the inclusion of new individuals and entities, the overall structure and intent of the sanctions has remained the same.[1]

In February 2022, following the Russian military intervention in Ukraine, the EU, the US, and other countries intensified their efforts by significantly increasing sanctions and coordinating their actions to enhance the effectiveness of the measures taken against Russia.[2] These measures were adopted in collaboration with G7 countries and other partners, such as Australia, South Korea, Norway and Switzerland, among others. Despite the selective nature of these sanctions, they may have a significant impact on Russia's economy, leading to economic weakening of the targeted country. Nevertheless, the objective of discouraging Russia from pursuing additional destabilising actions or stopping its aggression towards Ukraine has not yet been accomplished. As underlined by the Court of Justice of the European Union in *Rosneft*, the restrictive measures adopted against the Russian economy «plainly contributes to achieving the objective of increasing the costs of the Russian Federation's actions to undermine Ukraine's territorial integrity, sovereignty and independence, and of promoting a peaceful settlement of the crisis».[3]

2 Investment restrictions and export ban of technology

Technology and innovation, as well as foreign direct investment (FDI), play crucial roles in driving economic growth and development. Innovation is a driver of GDP growth because of increased productivity, enhanced competitiveness, creation of new industries and markets and, finally, spillover effects (innovations in one industry or sector can have effect on others).

It is, therefore, unsurprising that sanctions are utilised as a tool for political and economic leverage. The impact of sanctions on capital flows to and from Ukraine and Russia has been swift and substantial. The involvement of the business community in Russia-related trade has significantly decreased, with a substantial portion of this decrease being voluntary.[4] This deliberate choice by commercial actors to de-couple from

[1] The EU's measures that restrict certain activities or trade are established on the basis of two provisions, namely Article 29 of the Treaty on European Union and Article 215 of the Treaty on the Functioning of the European Union.
[2] For a general overview see Anna Caprile, Angelos Delivorias, '*EU sanctions on Russia: Overview, impact, challenges*', European Parliamentary Research Service (EPRS), PE 739.366 – March 2023.
[3] Case C-732/18 P, *PAO Rosneft Oil Company and Others v Council of the European Union* [2020] [92].
[4] See Richard L Kilpatrick Jr, 'Self-sanctioning Russia' (EJIL: Talk!, Blog of the European Journal of International Law, 11 May 2002) <https://www.ejiltalk.org/self-sanctioning-russia/> accessed 29 March 2023.

Russia-linked transactions, in addition to the rapid and comprehensive economic sanctions imposed by major powers such as the EU, UK, US, and Japan, has considerably strengthened the collective response against Russia's actions. Additionally, divestments resulting from these sanctions are expected to exacerbate the decade-long trend of declining investment in Russia.[5]

Technology and innovation play several key roles in the strategies used to weaken the economy of the Russian Federation ("economic warfare"). One of the most notable examples occurred when major Russian banks were disconnected from specialized financial messaging services, such as SWIFT (Society for Worldwide Interbank Financial Telecommunication), during the enforcement of the third package of EU sanctions (28 February 2022).[6] Technology can pave the way for innovative economic instruments, such as cryptocurrencies, which can be utilised to bypass sanctions and enable international financial transactions through non-traditional channels. The EU's eighth package (6 October 2022) imposed a complete prohibition on crypto-asset wallets and sanctions on the provision of information technology (IT) and IT consultancy services. At the same time, it is worth noting that cryptocurrencies have been used as a useful tool for transferring money to Ukraine.[7]

Extensive economic sanctions can result in adverse consequences for technological progress and ability to compete at global level. In the case of Russia, the primary objective of these restrictions was to limit its technological development and ability to use technology for harmful purposes, particularly in the context of the conflict in Ukraine. Such sanctions can also contribute to restricting the spread of weapons and impeding the advancement of sophisticated military capabilities by the Russian Federation. Arms embargoes and restrictions on other trade, such as exporting technology required for oil exploration, were also imposed on Russia to disrupt its trade and economic activities. These measures were intended to limit Russia's ability to build up its military capabilities and exploit its natural resources.

In response to Russia's annexation of Crimea and the subsequent military conflict in eastern Ukraine from 2014, various countries, such as the United States, the European Union (EU), and Canada, imposed unilateral economic sanctions that restricted the export and re-export of technology to the Russian energy sector (prohibiting exports to Russia of goods and technologies in the oil-refining sector and prohibiting new investments in the

[5] OECD, *International investment implications of Russia's war against Ukraine* (OECD Publishing, 4 May 2022) 13-14 <https://doi.org/10.1787/a24af3d7-en> accessed 29 March 2023. In these circumstances, Russia may try to Invest in education and workforce skills, stimulate innovation and technological progress, diversify the economy, and develop the domestic market, promote trade with countries which are not applying sanctions, implement structural reforms.

[6] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) serves as an international provider of secure financial messaging services, connecting over 11,000 banks across the globe. As a cooperative society governed by Belgian law, it is owned by its member institutions and maintains its headquarters in Belgium.

[7] Cristina Criddle and Joshua Oliver, 'How Ukraine embraced cryptocurrencies in response to war', *Financial Times* (London, 19 March 2022) <https://www.ft.com/content/f3778d00-4c9b-40bb-b91c-84b60dd09698> accessed 29 March 2023.

Russian energy and mining sector) and defence sector (prohibiting export to Russia of dual-use goods/technology, arms, civilian firearms, ammunition, military vehicles, paramilitary equipment and banning certain exports in the aviation, maritime, and technology sectors). However, the formulation of these sanctions was vague, and they contained loopholes that were exploited.[8]

The EU's 9th (16 December 2022) and 10th (25 February 2023) packages of sanctions introduced and expanded new export controls and restrictions on dual-use goods and technology.[9] In order to restrict trade with Russia, specific measures were implemented, including restrictions on the export of crucial technologies and components to key technological sectors. The EU has taken significant measures to restrict trade with Russia by expanding the list of entities connected to Russia's military and industrial complex and imposing further export bans on critical technology and industrial goods (electronics, telecommunications, and aerospace). The export ban on aviation- and space-industry-related goods and technology has been extended to include aircraft engines and their parts, which applies to both manned and unmanned aircraft.[10] Additionally, new electronic components, rare earth materials, electronic integrated circuits, and thermal cameras that can be used in Russian weapons systems have been added to the list of restricted items that could contribute to the technological enhancement of Russia's defence and security sector.

3 The implementation of sanctions: technology and info-sharing and new proposals

The implementation of sanctions by EU Member States can vary, leading to inconsistency in their application. The EU sanctions are adopted by the EU Council through decisions and regulations that are directly applicable. However, Member States are responsible for implementing the sanctions, enforcing them in case of violation, and designating competent authorities. When appropriate, States can establish regulations to

[8] See Irina Bogdanova, 'The Role of Technology Sanctions in Crippling Russia's War Machine' (IISD,26 September 2022) <https://www.iisd.org/articles/policy-analysis/technology-sanctions-russia-war> accessed 29 March 2023 and James Byrne and others, 'Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine' (RUSI, 2022), <https://static.rusi.org/RUSI-Silicon-Lifeline-final-web.pdf> accessed 29 March 2023; Michael Adam and Sanne Keijer, 'Sanctions on the Russian digital sector: How effective are they?' (European Parliamentary Research Service (EPRS), PE 739.320, February 2023); Andrei Panibratov, 'Sanctions, cooperation, and innovation: Insights into Russian economy and implications for Russian firms' (2021) 2(3) BRICS Journal of Economics 4.

[9] Council of the EU, 'One year of Russia's full-scale invasion and war of aggression against Ukraine, EU adopts its 10th package of economic and individual sanctions' (25 February 2023) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/16/russia-s-war-of-aggression-against-ukraine-eu-adopts-9th-package-of-economic-and-individual-sanctions/> accessed 29 March 2023 and Council of the EU, 'Russia's war of aggression against Ukraine: EU adopts 9th package of economic and individual sanctions' (16 December 2022) <https://www.consilium.europa.eu/en/press/press-releases/2023/02/25/one-year-of-russia-s-full-scale-invasion-and-war-of-aggression-against-ukraine-eu-adopts-its-10th-package-of-economic-and-individual-sanctions/> accessed 29 March 2023.

[10] The EU imposed sanctions on Iranian arms manufacturers and individuals for providing drones to Russia in the 10th package.

suspend the financial operations and economic assets of persons and organizations subject to restrictive actions at a national level. This can be carried out through administrative freezing measures, judicial freezing measures, or equivalent methods.

Technology can assist governments in enforcing sanctions by providing innovative ways for information sharing and cooperation. Governments can leverage several technological tools to share information and coordinate actions more efficiently and effectively. Information sharing between countries is also critical to ensure that sanctions are applied in a uniform way.[11]

The European Commission oversees the implementation and enforcement of EU sanctions in the Member States. Given the complexity and variety of sanctions adopted against Russia within such a short period of time, it is perhaps not surprising that the Commission has set up a website for anonymous reporting of suspected violations of the sanctions (EU Sanctions Whistleblower Tool).[12]

To ensure effective implementation of sanctions, coordination bodies have been established. One such example is the European Commission's "Freeze and Seize" Task Force, which was created to facilitate EU-level coordination in implementing sanctions against listed Russian and Belarusian oligarchs.[13] The task force is working alongside the newly established 'Russian Elites, Proxies, and Oligarchs (REPO)' Task Force, under which the EU operates together with the G7 countries, i.e. Canada, France, Germany, Italy, Japan, the United Kingdom and the United States, as well as Australia.[14]

To streamline and simplify the implementation of financial sanctions relating to the Common Foreign and Security Policy (CFSP), various banking organisations within the European Union recognised the need for a consolidated list of individuals, groups, and entities subject to these sanctions. This list could help facilitate compliance with financial sanctions and reduce the risk of inadvertently facilitating prohibited financial transactions.[15] The European Banking Federation, the European Savings Banks Group, the

[11] The EU-US Trade and Technology Council functions as a platform for the United States and European Union to harmonise their approaches to crucial global trade, economic, and technology matters. It was established during the EU-US Summit on June 15, 2021 in Brussels, cf <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en> accessed 29 March 2023.

[12] Cf <https://eusanctions.integrityline.com> accessed 29 March 2023.

[13] See the Ministerial Joint Statement of 17 March 2022 on the Russian Elites, Proxies, and Oligarchs Task Force by the European Commission, the United States, Australia, Canada, France, Germany, Italy, Japan and the United Kingdom <https://ec.europa.eu/commission/presscorner/detail/en/statement_22_1850> accessed 29 March 2023. The 'Freeze and Seize' Task Force is comprised of the European Commission, national contact points from each EU member state, as well as various other EU agencies and bodies as necessary, including Eurojust and Europol. Its main objective is to coordinate actions by EU member states, Europol, Eurojust, and other relevant agencies in order to seize and potentially confiscate assets of Russian and Belarusian oligarchs. The European Commission provides strategic coordination, the operational coordination is of Europol and Eurojust.

[14] Russian Elites, Proxies, and Oligarchs Task Force Joint Statement (US Department of the treasury, 29 June 2022) <https://home.treasury.gov/news/press-releases/jy0839> accessed 29 March 2023.

[15]<https://www.eeas.europa.eu/eeas/european-union-sanctions> The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has developed a system called "OFAC Online" that allows individuals and businesses to search a consolidated database of sanctioned individuals and entities, making it easier to comply with sanctions regulations (<https://sanctionssearch.ofac.treas.gov/> accessed 29 March 2023).

European Association of Co-operative Banks, and the European Association of Public Banks, commonly referred to as the EU Credit Sector Federations, collaborated with the Commission to establish this consolidated list. The Commission is responsible for hosting, maintaining, and regularly updating the database containing such list (Financial Sanctions Database - FSF platform).[16]. The primary aim of the consolidated list was to assist members of the EU Credit Sector Federations in complying with CFSP-related financial sanctions. Financial institutions can avoid engaging in prohibited transactions and potential penalties for non-compliance by accessing an updated list of individuals, groups, and entities that are subject to sanctions. Additionally, the consolidated list is a valuable resource for governments to monitor and enforce financial sanctions against targeted individuals and entities. Overall, the creation of a consolidated list of those subject to CFSP-related financial sanctions is a vital measure in implementing and enforcing sanctions. This effort provides more clarity and guidance to credit and financial institutions in their compliance efforts and strengthens the ability of governments to prevent illicit activities from being funded.

Just recently, it has been reported that the G7 countries have decided to develop a new mechanism called the "Enforcement Coordination Mechanism" to improve the enforcement of existing sanctions on Russia. This tool can be seen as a means to enhance coordination and collaboration in the realm of sanctions by exchanging intelligence and information pertaining to suspected sanction violations. This is essential in building a stronger case against the individuals involved and can help refine the process of acting against violators, ultimately increasing the effectiveness and efficiency of the measures in the long run.[17]

Furthermore, the European Commission has proposed to harmonise criminal offences and penalties for violating EU restrictive measures to ensure their full implementation. The harmonisation of EU rules will make it easier to investigate, prosecute and punish violations of restrictive measures across all Member States. The European Commission has proposed a list of criminal offenses that violate EU sanctions. These measures include various actions such as making funds available to designated entities, failing to freeze these funds, allowing designated individuals to enter or transit through EU Member States, engaging in prohibited transactions with third countries, trading in restricted goods or services (such as technology), and providing financial or other services that are prohibited or restricted. The offenses also cover attempts to circumvent restrictive measures by concealing funds or ownership.[18] Additionally, the Commission is proposing stricter

[16] DG FISMA, 'Financial Sanctions Database - FSF platform'.
[17] Alberto Nardelli and Jennifer Jacobs, 'G-7 Set to Create New Tool to Bolster Enforcement of Russia Sanctions' (*Bloomberg*, 22 February 2023) <https://www.bloomberg.com/news/articles/2023-02-22/g-7-readies-new-tool-to-bolster-enforcement-of-russia-sanctions> accessed 29 March 2023.
[18] See the Proposal for a Directive of the European Parliament and of the Council on the definition of criminal offences and penalties for the violation of Union restrictive measures, COM (2022) 684 final [2022].

regulations on asset recovery and confiscation, which will aid in enforcing EU restrictive measures and will guarantee the efficient tracking, freezing, handling, and seizure of profits obtained from breaking such measures.[19]

[19] See Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation, COM(2022) 245 final [2022].

*Chiara Ferri**

INTERNATIONAL TIMBER TRADING UNDER SANCTIONING REGIMES: THE ROLE OF TECHNOLOGICAL INNOVATION

Abstract

This paper examines how the forest sector is affected by the sanctioning regimes created by governments to deal with ongoing international emergencies and which role innovation and technology could play in implementing restrictive measures. Particularly referred to as international trading, one of the sectors affected by restrictive measures is the forest industry, specifically importing and exporting timber. The first part focuses on the current legislative framework of the European Union to pinpoint the critical regulatory issues under consideration and, given the information mentioned above, the flaws in the sanctioning regimes. The second part, more in-depth, introduces innovation and technology (e.g., blockchain) as a tool that can be used to implement the regulatory design of economic sanctions. By analysing the current use of blockchain in the forest industry, this paper tries to identify its potential and any problematic issues that could arise to hypothesise future research activities.

JEL CLASSIFICATION: K23, K33, K39

SUMMARY

1 Foreword

As emerged with the pandemic, the global economy is strictly connected. As withCovid-19 new events address how alternative measures could be taken to promote political action. The existence of restrictive government sanctions implies the analysis of their design and effectiveness. I have chosen to investigate the forest industry to see if the sanctions applied from the Russian-Ukrainian crisis are currently being respected,

* PhD candidate in Blockchain & DLT, University of Camerino, and member of BABEL-Blockchains and Artificial intelligence for Business, Economics and Law, Department of Economics and Management, University of Florence.

considering some sanctioning packages in force and being the wood one of the raw materials prohibited from import.[1]

This decision has impacted the organisation of markets. It has again been emphasised how governments are (willingly or unwillingly) linked to one another in many ways. While these connections undoubtedly bring advantages, the complexity of managing trade flows has become apparent, especially when it is necessary to interrupt some of them. From this point, it becomes clear the need of a better understanding of the existing laws and regulations about timber trading to focus on how the new restrictive economic measures could be applied.

It has been reported that significant violations of the legislative frameworks are currently in force, not only regarding the restrictive measures recently enacted but even with regards to the sector-specific rules. From this perspective, it is even more crucial to study the possibility of new technologies that can be used as innovative tools to ensure the respect of the regulations. Considering that blockchain is already used and studied in the forest industry it will be examined here with specific reference to the transparency and traceability of the timber supply chain.

2 The timber industry: an emblematic sector

Some of the economic provisions under consideration concern the retrieving of raw materials which are fundamental to productive processes. It affects the economies of those governments, which are pointed out as the illegal triggers of a conflict. This means that not only is their industry affected but also their arsenal and limiting their finances doomed to subsidize the conflict.

The European Union deemed it necessary to draw several sanctions that would weaken Russia's economic basis by depriving it of crucial technologies and markets and significantly reducing its ability to run the conflict through restrictions on import and export.[2] Later, in light of its involvement in Russia's military invasion of Ukraine, the

[1] On 24th February 2022, following a decision by President Vladimir Putin, Russia militarily attacked Ukraine and invaded the border territories, subsequently declaring the annexation of the Ukrainian regions of Donetsk, Luhansk, Zaporizhzhia and Kherson to its nation. This resulted in a conflict that, to date (February 2023), has unfortunately not found a solution yet. The Russian-Ukrainian conflict immediately brought to the attention of international diplomacy the thorny question of the most effective ways to react. Not being able - or willing - to act militarily, the choice turned to economic sanctions. However, some countries abstained in the March 2022 UN vote and have not adopted sanctions against Russia, just as others have declared themselves opposed to this course of action. See: United Nations, 'Ukraine: General Assembly Passes Resolution Demanding Aid Access by Large Majority' (24 March 2022) UN News <https://news.un.org/en/story/2022/03/1114632> accessed 10 October 2022; Filippo Mastroianni, 'Dalla Prima Risoluzione ONU alle Sanzioni. Quattro Mappe per Aiutarci a Capire la Percezione dell'invasione Russa in Europa' (3 June 2022*)* Il Sole 24 Ore Info Data <www.infodata.ilsole24ore.com/2022/06/03/dalla-prima-risoluzione-onu-alle-sanzioni-quattro-mappe-per-aiutarci-a-capire-la-percezione-dellinvasione-russa-in-europa/> accessed 10 October 2022.

[2] To have a comprehensive view of restrictions imposed by European Union, see: European Council, 'Timeline - EU Restrictive Measures against Russia over Ukraine' <www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/>, accessed 18 February 2023.

European Union decided to draw sanctions now against Belarus.[3] We must wonder if sanctions have been complied with after issuance, and if not, what can be done to ensure compliance. Furthermore, the above is necessary not only to penalize those who deliberately decide to act in violation of the imposed bans but also to ensure that there is correct information on market operators in compliance, and, above all, if it is desirable to reward those who, conversely, act following the regulations. Firstly, this analysis aims to identify the characteristics that distinguish a specific sector and then outline a scheme of action that can be applied to other realities.[4]

Emblematic in our research is the timber sector. To make a better comprehension of the highlighted phenomenon a brief overview on the regulation in force within the European Union could be useful. In 2005, the member States of the European Union agreed on establishing a licensing system for timber import to oppose the illegal logging and associated trade, named Forest Law Enforcement, Governance and Trade (from now on referred to as FLEGT).[5]

The FLEGT establishes a licensing system for timber imports within the European Union market, with documents that certify the conformity of a timber shipment with the regulatory requirements in force in the country of origin. The verifiability and non-falsifiability of these documents are to be guaranteed.[6]

In its path and to strengthen its aim, the EU Member States agreed to issue the EU Timber Regulation No. 995/2010 (from now on EUTR), which came into force in 2013, aimed at reducing the devastating effects of the illegal timber trade.[7] The EUTR underlines that the operators who place timber for the first time in the EU market must be under due diligence (while a trader in the supply chain should only be required to provide basic information) to enable the traceability of timber and timber products. Based on article 6 of EUTR, due diligence means that operators must fulfil three elements such

[3] See European Council, 'EU Restrictive Measures against Belarus' <www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-belarus/> accessed 8 October 2022.

[4] Sanctions can be divided into three macro-sectors: those affecting people - consisting of a travel ban on them and freezing their assets - and those affecting trade, in the dual direction of imports and exports. Therefore, European natural and legal persons are not allowed to sell certain products to Russia (export restrictions) or purchase them from Russia (import restrictions).

[5] Council Regulation (EC) 2173/2005 of 20 December 2005 on the establishment of a FLEGT licensing scheme for imports of timber into the European Union [2005] OJ L347/1.

[6] This system is based on Voluntary Partnership Agreements (VPAs) between European countries and timber-producing third countries that want to eliminate illegal logging and trade and facilitate access to their timber products to the European Union. Interested Parties are in fact required to register on an EU portal, from which it is possible to check the conformity with the legislative framework of the European regulations. Conformity is intended as completeness of the information required to obtain and to maintain the license to import products, its expiry date and the information needed to verify the cargo. See: Ministero dell'agricoltura della Sovranità Alimentare e delle Foreste, Regolamento FLEGT <www.politicheagricole.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/17201> accessed 10 October 2022.

[7] It prohibits illegally harvested timber, or products derived from such timber, from being placed on the market in the European Union, laying down the obligations of operators as well of traders. European Parliament and Council Regulation (EU) 995/2010 of the of 20 October 2010 laying down the obligations of operators who place timber and timber products on the market, Text with EEA relevance [2010] OJ L295/23.

as access to information, risk assessment and risk mitigation.[8] As to the access to information, the two main elements that must be proved are the country of harvest (where applicable also the concession of harvest) and all the necessary documents supporting the compliance of timber with applicable legislation.[9] Specifically stated by the aforementioned article, risk assessment procedures shall enable the operators to evaluate the risk of illegally harvested timber or timber products derived from such timber. For the purpose of this analysis, two of the listed criteria are undoubtedly relevant. Indeed, at the same time of the compliance of the products with the country of harvest applicable legislation, it must be considered also of the prevalence of armed conflict and the presence of sanctions imposed by the UN Security Council or the Council of the EU on timber import and export.[10] Both the FLEGT and the EUTR underline the importance of a continuous monitoring activity set by each Member State, which should interrupt the import of products if there is a lack of the mentioned prerequisites.

In light of the above, it is essential to recall Article 215 TFEU, where it is stated that it is possible to interrupt or reduce, in part or entirely, economic and financial relations with one or more third countries.[11] More in-depth, the Council of the European Union should adopt restrictive measures against natural or legal persons and groups or non-State entities.[12] In this sense, several timber-producing countries' institutional and management deficiencies in the Forestry Sector are of international concern: this has social, political, and economic implications. For instance, the latest Food and Agriculture Organization of the United Nations (FAO) report refers to 2019, when Europe imported forest products

[8] The trading under the EUTR required to act with due diligence, which can be identified in three key elements: 1) Information: this relates to the fact that economic operators must be able to have availability and access to information describing the type of timber or wood component of the product, the country where harvesting takes place, the species, the quantity, the details needed to identify the supplier and information relating to the National Legislation of the country of origin of the product; 2) Risk assessment: the trader must be responsible for the risk management of the product's entry into the market, for which easy access to the already mentioned information on the product's chain of custody is required, so that it is possible to verify its compliance with the criteria imposed by the legislation in force; 3) Risk mitigation: when, as a result of the above comparative assessment, it becomes apparent that timber may be among those for which an import ban applies, this risk must be assessed by requesting further verification, with the supplier providing additional information and documentation. Based on the above, the importance of transparency of the chain of custody and product traceability during the process of supply chain is evident. See: European Commission, 'Timber regulation' <https://ec.europa.eu/environment/forests/timber_regulation.htm> accessed 12 October 2022.

[9] Acting with due diligence requires the operator to ensure that timber purchases and related payments do not fall into the hands of one or more sanctioned parties or entities directly or indirectly. Indeed, the primary intent of economic sanctions is to weaken the State subject to restrictions, preventing it from having the materials and money to continue its aggressive policies. This applies to public entities as well as to companies and individuals who own or control a company or corporation as this is considered as a mode of indirect financing. In doing so, operators can use all the already good known practices and certification of third-party verification schemes as well, including those who include verification of compliance with applicable legislation. See: European Commission, 'Eighth Meeting of the "Multi-Stakeholder Platform on Protecting and Restoring the World's Forests, including the EUTR/FLEGT" With a focus on the implementation of the EUTR and FLEGT Regulation' (16 March 2022) <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings?lang=en> accessed 14 October 2022.

[10] European Parliament and Council, Regulation (EU) 995/2010, art 6 (1) letter b).

[11] European Union, Consolidated Version of The Treaty on The Functioning of The European Union [2012] OJ C326/47.

[12] At the same time, article 29 of the Treaty of the European Union needs to be recalled. See: European Union, Consolidated Version of the Treaty on European Union [2008] OJ C115/13.

totalling USD 107.656,890. The Russian Federation was the world's leading exporter of softwood timber.[13]

Therefore, it is not surprising that the EU has also identified timber as one of the production sectors to which the abovementioned import restrictions should be applied. The armed conflict between Russia and Ukraine creates a complex scenario which needs to be dealt according to the European legislative framework. This is why several acts have been issued.

2.1 The sanctioning regimes in force

In summary, it is possible to confirm that, given the current disposition, it is not now possible to import timber or timber products harvested in some regions of the EU into the market, one of which is Russia. These restrictions stem from the first decisions of the EU, dating back to 2014 when Russia illegally annexed the Crimean territories.[14] This first approach to the sanctioning regime prohibited selling, supplying, transferring, or exporting, directly or indirectly, dual-use goods and technology. In contrast, those items were or may be intended, in their entirety or part, for military use or a military end-user.

After the military invasion of the Ukrainian territories occurred on 24th February 2022, the EU confirmed its sanction measures in meetings on 2nd March 2022 and 8th April 2022, which included a ban on the import of all timber and timber products from the territories of Russian and Belarus in the light of the continuation of the conflict. The sale, supply, transfer, or export of goods which could contribute to the enhancement of Russian industrial capacities to any natural or legal person, entity or body in Russia or for use in Russia is now prohibited based on article 3k of the Council Regulation 2022/576, amending the restriction issued in 2014. This includes goods such as wood according to the Combined Nomenclature, which is listed in annex XXIII.[15]

[13] Forest products in this case must be considered as all Roundwood felled or otherwise harvested and removed. It comprises all wood obtained from removals, i.e., the quantities removed from forests and from trees outside the forest, including wood recovered from natural, felling and logging losses during the period, calendar year or forest year. It includes all wood removed with or without bark, including wood removed in its round form, or split, roughly squared or in another form (e.g., branches, roots, stumps, and burls (where these are harvested) and wood that is roughly shaped or pointed. In the removal statistics, it represents the sum of wood fuel; saw logs and veneer logs; pulpwood, round and split; and another industrial Roundwood. The trade statistics represent the sum of industrial Roundwood, and wood fuel. See FAO, 'Yearbook of Forest Products' (2021) <www.fao.org/forestry/statistics/80570/en/> accessed 11 October 2022. The FAO Yearbook of Forest Products is a compilation of statistical data on basic forest products for all countries and territories of the world. It contains series of annual data on the volume of production and the volume and value of trade in forest products. It includes tables showing direction of trade and average unit values of trade for certain products.

[14] Even if this approach initially didn't focus on timber and timber products, it is therefore important to pinpoint the timeline of the current measures in force. See: Council Regulation (EU), No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2014] OJ L229/1.

[15] The Combined Nomenclature (CN) is a tool for classifying goods, set up to meet the requirements both of the Common Customs Tariff and of the EU's external trade statistics. See: Council Regulation (EU) 2022/576 of 8 April 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L111/1.

As mentioned, some restrictive measures also concerned Belarus.[16] Regarding the Council Regulation 2022/355, it is prohibited to import, directly or indirectly, wood products which originated or were exported in Belarus, to purchase, directly or indirectly, wood products and transport wood products.[17] Confirming the commonality of intent that emerged following the start of the war conflict, the EU Member States confirmed that restrictive measures, or sanctions, are essential to the European Union's Common Foreign and Security Policy. They are used by the institutions when it is necessary to respond to an event that could destabilise European interests and the values of its internal and international policy.

This statement is supported by the fact that Russia is not the only one to have been subjected to such proceedings. Actually, EU has also subjected Iran, North Korea, and Myanmar to sanction procedures.[18] The last mentioned is of particular importance for this analysis, as discussed below, in order to examine how technology could be used to follow international timber trading. As an exporter of valuable timber (teak and others) explicitly used in shipbuilding, Myanmar has been affected by European sanctions - and not only European - following the military coup d'état perpetrated in February 2021.[19] In this case, the European Union has also introduced a progressive number of sanctions that – to date have reached the fifth cycle - due to the prolonged state of human rights violations.

Having regard to Council Regulation 401/2013, with the Council Implementing Regulation 2021/998, the EU decided to amend the list of entities addressed by the restrictive measures.[20] In synthesis, we note economic restrictions based on the timber trade and the legal entities operating in the production sector. The abovementioned is extremely important as it is possible to think of the multiple geographical and commercial

[16] Council Regulation (EU) 2022/355 of 2 March 2022 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus [2022] OJ L 67/1.

[17] The most recent consolidation of the imposed sanctions was ordered at the Council Meeting dated 6th October 2022, confirming the ban on importing all types of wood products from the territories of Russia and Belarus. See: Council Regulation (EU) 2022/1903 of 6 October 2022 amending Regulation (EU) 2022/263 concerning restrictive measures in response to the recognition of the non-government controlled areas of the Donetsk and Luhansk oblasts of Ukraine and the ordering of Russian armed forces into those areas [2022] OJ L259/65, 1; Council Regulation (EU) 2022/1904 of 6 October 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L259/65, 3; Council Regulation (EU) 2022/1905 of 6 October 2022 amending Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine [2022] OJ L259/65, 76; Council Implementing Regulation (EU) 2022/1906 of 6 October 2022 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine [2022] OJ L259/65, 79.

[18] European Council, 'Iran: EU restrictive measures' (2022) <www.consilium.europa.eu/en/policies/sanctions/iran/> accessed 10 November 2022; European Council, 'EU restrictive measures against North Korea' (2022) <www.consilium.europa.eu/en/policies/sanctions/history-north-korea/> accessed 10 November 2022.

[19] For an overview of multilateral and unilateral economic and financial sanctions, see: Fabio Cozzi, 'Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?' (2020) 20(2) Global Jurist <www.degruyter.com/document/doi/10.1515/gj-2019-0047/html> accessed 18 January 2023.

[20] See: Council Implementing Regulation (EU) 2021/998 of 21 June 2021 implementing Regulation (EU) No 401/2013 concerning restrictive measures in view of the situation in Myanmar/Burma [2022] OJ L219 I/45; Council Regulation (EU) No 401/2013 of 2 May 2013 concerning restrictive measures in view of the situation in Myanmar/Burma and repealing Regulation (EC) No 194/2008 [2013] OJ L121/2013.

transfers and products. As mentioned, nowadays, it is correct to discuss the trade of timber – considered a raw material – as for products made of forest materials. In this sense, it may be strengthened as wood products are increasingly subject to certification and inspection procedures.[21]

Since timber from Russia, Belarus and Myanmar is now considered 'conflict timber' and, as such, is subject to restrictions on its use, it is necessary to identify the origin of a timber consignment. If it comes from these countries, not only is its direct import forbidden but also its use. Moreover, for those who contravene these guidelines it is forbidden to certify and market its derivatives.

The abovementioned circumstance must be read in the light of two certification programs, the Forest Stewardship Council (FSC) and the Programme for the Endorsement of Forest Certification (PEFC), deemed necessary to suspend their certification operations in the Russian and Belarusian territories.[22]

Consequently, as of 2nd March 2022, all wood from these territories can no longer be used in certified production.[23] All the certification schemes stressed the importance of the chain of custody, but the issues concerning supply chains involve different aspects.[24] It is evident how the processes affecting the product could become opaque when becomes multistage, involving several geographically dispersed entities in distant locations. As a result, the traceability of the product itself suffers or is wholly undermined. In the same vein, as the wood comes from Russia and Belarus, it is important to consider similar situations which apply the same model.

2.2 International timber trading in light of the sanctioning regimes

In this context, the value of the regulations and the significant impact of the sanctions on the global timber market are clear. However, two logically consecutive and interlinked

[21] Nathan Iben, Christian Pilegaard Hansen and Benjamin Cashore, 'Timber legality verification in practice: Prospects for support and institutionalization' (2014) 48 Forest Policy and Economics.

[22] The Forest Stewardship Council A. C. (FSC) is an international non-profit, multistakeholder organization established in 1993 that promotes responsible management of the world's forests via timber certification and held by forest owners, timber industries, social groups, and environmental organizations to come together to find solutions to improve forest management practices. Its work is carried forward six primary areas, namely forests, chain of custody, social policy, monitoring and evaluation, quality assurance, and ecosystem services, in order to fight against illegal logging, deforestation and global warming. The Programme for the Endorsement of Forest Certification (PEFC) is an international, non-profit, non-governmental organization which promotes sustainable forest management through independent third-party certification. It is considered the certification system of choice for small forest owners. Based in Geneva (Switzerland) and founded in 1999, nowadays it represents more than 299.99 million hectares of certified forests that is about two-thirds of the globally certified forest area. It is correct to underline that mutual recognition of FSC and PEFC certified material in the chain of custody has not yet happened and some non-governmental organization such as Greenpeace does not recognize PEFC as an alternative to FSC.

[23] 'Timber from Russia and Belarus considered conflict timber' (4 March 2022) <https://pefc.org/news/timber-from-russia-and-belarus-considered-conflict-timber> accessed 14 October 2022.

[24] As far as trade is concerned, one of the supply chain central elements is how is possible to check the way in which a X product arrives at point Y, be it a finished product to be placed on the distribution market for the end consumer, or a semi-finished product that passes from one stage of processing to another, or even simply a product that has to be transferred from one point to another.

questions must be raised. The first concerns the effectiveness of the sanctions applied.[25] To date, can we say that they have been respected and, therefore, efficiently implemented?[26] The second, in the case of a negative answer to the first question, is there a technology that can be used to remedy the system's deficiency?

It is necessary to preface that even if EU timber restrictive measures against Russia and Belarus have recently been developed, is still lack of official reports regarding their effectiveness. Nevertheless, thanks to the Environmental Investigative Agency (from now on EIA), one of the organisations working to verify compliance with regulations to protect and safeguard the environment, it is possible to identify some breaches in the system.[27]

The decision to take into account is not only the sanctioning regimes against Russia and Belarus, but also to Myanmar, is based on the necessity to search for a possible plan of action. As analysed below with Myanmar timber trading and then with a report on the American imports, it will be possible to stress a recurring scheme that presupposes using new technological tools.

Regarding the restriction of timber - mainly teak - from Myanmar, the EIA shows how it is still acting in open violation of the sanctions imposed on that State, and not only after the coup d'état in February 2021. It is believed that even before that date, when it had already been established that environmental protection issues meant that the teak produced could not meet the EU entry requirements under the EUTR, some realities acted in violation of the EU Law. [28]

[25] For an interesting reading on the effectiveness of sanctions, their nature, and the purpose of punishment, see: Kim Richard Nossal, 'International Sanctions as International Punishment' (1989) 43(2) International Organization 301.

[26] It is important to stress that on the 25 May 2022 European Commission presented a proposal for a decision to extend the list of these areas of crime to include the violation of restrictive measures adopted by the European Union. The proposal is to consider the violation of Union restrictive measures as an area of crime within the meaning of Article 83(1), second subparagraph, TFEU. In the light of the above, the importance to define the compliance with restrictive measures in specific sectors is undeniable. See: Council of the European Union, Interinstitutional File 2022/0176 (NLE) <https://data.consilium.europa.eu/doc/document/ST-10287-2022-REV-1/en/pdf> accessed 02 December 2022.

[27] The Environmental Investigative Agency is a London-based agency, investigating and campaigning against environmental crime and abuse. See: <https://eia-international.org/>.

[28] See: Environmental Investigation Agency, 'German firm investigated by EIA convicted for breaking EU sanctions by trading illegal Myanmar teak' (EIA 28 April 2021) <https://eia-international.org/news/german-firm-investigated-by-eia-convicted-for-breaking-eu-sanctions-by-trading-illegal-myanmar-teak/> accessed 22 September 2022, in which the agency shows as the District Court of Hamburg at the beginning of 2021 sentenced the company WOB Timber GMBH to pay €3.3 million for violation of the Union law, while the Managing Director received a (suspended) 21-month prison sentence and a €200,000 fine for illegally importing teak from Myanmar between 2008 and 2011. Similarly, in a different briefing note, the EIA shows how the competent Dutch authorities have taken numerous actions against various European importers and traders who were responsible for illegal timber trafficking. In the course of the proceedings against them, it emerged that they had brought more than five hundred cubic meters of teak into the European market, with an estimated value of more than three million dollars. See: Environmental Investigation Agency, 'Dutch traders exposed by EIA are facing legal action for importing illicit teak from Myanmar' (EIA 8 April 2021) <https://eia-international.org/news/dutch-traders-exposed-by-eia-are-facing-legal-action-for-importing-illicit-teak-from-myanmar> accessed 10 October 2022. It should be recalled that the EU Legislation generally prohibits the use of timber harvested in unauthorized areas or war zones and, if timber is found to be harvested, processed, or manufactured in such areas, this affects the legality of the timber and would likely lead to the impossibility to carry out an appropriate Due Diligence Assessment, and thus, incompliance with Article 4(2) in accordance with Article 6(1) of the EUTR. This could also lead to a breach of Article 4(1) of the EUTR which prohibits placing on the EU market of illegally harvested timber or timber products.

In the September 2021 report entitled "The Italian Job", the EIA points out that after the coup d'état and the sanctions enacted, timber still manages to reach the rest of European countries precisely via Italy (which has been the largest importer of wood products from Myanmar since 2013) in violation of EU regulations.

The situation in Myanmar has also been analysed by the World Conservation Monitoring Centre of the United Nations Environment Programme (UNEP-WCMC), which, in its briefing of April 2022, refers to a report in which the military junta claims to have auctioned more than $8 million worth of teak and exported more than $190 million of wood products since the coup d'état.

Importers from the European Union (mainly Italy, but also those from other EU member states) and importers from the United States, the United Kingdom, Switzerland, and Canada, have all been identified as having also imported timber in violation of the sanctions in force since 2021. [29]

An exciting report issued by EIA in the past few days shows even more how even the government of the United States continues to import teak.

Between 1st February 2021 and 10th November 2022, 2.561 tons of teak were imported directly from Myanmar into the United States. [30]

It is undoubtedly due, at least in part, to deliberately illegal activity. Still, we can speculate that greater tracking information functionality could increase adherence to due diligence and make it easier to sanction non-compliance.

Since the restrictive measures regarding Russian and Belarusian timber are – so to speak – new, then we need more time to have official reports discussing their effectiveness.[31]

The EIA published an interesting report on the timber trading between Russia and the United States. The Agency believes that the government of the United States is continuing to import Russian timber in violation of the sanctions imposed. In particular, the findings published by EIA suggest that the United States is failing in its monitoring of imports - and,

[29] Environmental Investigation Agency, 'The Italian Job How Myanmar timber is trafficked through Italy to the rest of Europe despite EUilaws' (EIA 1 September 2021) <https://eia-international.org/wp-content/uploads/The-Italian-Job-2021-SPREADS.pdf> accessed 14 October 2022.

[30] In October 2022, 263.70 tons of teak were imported into the US via 14 shipments. A report written and edited by the Environmental Investigation Agency (which has been produced with the financial assistance of the Norwegian Agency for Development Cooperation (Norad) and the Foreign, Commonwealth and Development Office (FCDO), see: Environmental Investigation Agency, 'How US traders are ignoring sanctions to import conflict teak from Myanmar' (EIA December 2022) <https://eia-international.org/wp-content/uploads/Acts-of-Defiance-2022-SPREADS.pdf> accessed 8 December 2022.

[31] To date, it is possible to read some reports from investigative agencies that assert as the illegal timber is nowadays into the European market. See: Olga Ratmirova, Kseniya Viaznikoutsava and Alexander Yarashevich, 'Bypassing the sanctions Belarusian wood enters the EU under sham papers' 20 December 2022, <https://investigatebel.org/en/investigations/belaruski-les-abyhodzic-sankcyi-pa-falshyvyh-dakumentah> accessed 5 January 2023; Sarunas Cerniauskas, 'Traders Are Sneaking Banned Russian and Belarusian Wood into the EU By Pretending It's from Central Asia', 20 December 2022, <www.occrp.org/en/investigations/traders-are-sneaking-banned-russian-and-belarusian-wood-into-the-eu-by-pretending-its-from-central-asia> accessed 5 January 2023.

in this case, with its compliance with the Lacey Act[32] - concerning the mandatory requirement for importers to declare the country of harvest.[33]

The EIA data show that, besides Russia, the USA imported a considerable amount of timber from Asian countries such as China, Vietnam and Indonesia, which were not subject to the sanctions of the Russian-Ukrainian war.

It should be emphasised that, in the aftermath of the import restrictions from Russia, timber from these Asian countries increased by more than 200%.

Discarding the hypothesis that these States had such availability of indigenous timber, the EIA argues that the products arriving on the US market today are composed of Russian wood, which entered America by exploiting the loopholes in the traceability and transparency system of the supply chain in Asian countries.[34]

As the economy's structure changes, the leading roles, rules, and tools of the transnational exchange of goods cannot fail to change.[35]

Given the increasing complexity of markets, the supply chain is also noticing the emergence of new and different interlinked aspects, which make it more difficult not only to track the transactions performed efficiently but also the chain of custody of the products themselves, as well as the evaluation of this information.[36]

[32] Lacey Act, 16 U.S. Code § 3372. Reference to the Lacey Act is necessary as a result of the amendment passed on 22nd May 2008, which broadened the scope of the original 1900 Statute designed fundamentally for ecological protection purposes that prohibited the importation, exportation, transportation, sale, receipt, acquisition or purchase via interstate or foreign commerce of any animal or plant taken in violation of the laws of the United States or other countries, and now covers a wider range of products and in particular timber from 'illegal logging practices'. The 2008 Amendment to the Lacey Act, as mentioned earlier, was aimed precisely at avoiding this issue by considering - and still finding, given that it is still in force today - that it was necessary to focus on highlighting what had not been considered until then, i.e., that importers should indicate the imported species and the place of harvest.

[33] Environmental Investigation Agency, 'How Russian Conflict Birch Makes its Way to American Consumers' (30 September 2022), <https://us.eia.org/report/20220930-russian-conflit-birch/> accessed 14 October 2022. One of the primary objectives on which governs agreed on to implement policies to safeguard and combat non-legal logging. The Conference of the Parties is the governing body of the Convention on Biological Diversity, signed in 1992 by 150 government leaders and aimed to promote nature and human well-being. Currently the Convention has 196 Parties (all the countries that have either ratified, acceded to, approved, or accepted the Convention are therefore Parties to it). The United Nations Framework Convention on Climate Change is an international environmental treaty established to combat dangerous human interference with the climate system, entered into force on 21 March 1994.

[34] This consideration is supported by the China's current forestry policy, which aims at carbon neutrality and thus expansion and improvement of the forest area, and the fact that the traced supply chain concerns timber that grows in cold climates. In the report, the investigators quote a statement from an exporter who affirms: 'The way we are doing now is importing Russian birch to China first (it used to go from Russia directly to Vietnam), repackaged in China, and then re-exported to Vietnam. In doing this, the products exported to Vietnam cut all ties with Russia. The country of origin will be here [China]'.

[35] Cristina Poncibò, 'Lex Mercatoria ex Machina' (2021) 3 MediaLaws <https://www.medialaws.eu/rivista/lex-mercatoria-ex-machina/> accessed 27 September 2022.

[36] Mahtab Kouhizadeh, Sara Saberi and Joseph Sarkis, 'Blockchain Technology and the Sustainable Supply Chain: Theoretically Exploring Adoption Barriers' (2021) 231 International Journal of Production Economics <www.sciencedirect.com/journal/international-journal-of-production-economics> accessed 10 October 2022. The above is part of a broader debate on the design of so-called Industry 4.0, which relies heavily on the adoption and use of numerous technologies that enable the real-time collection, sharing, and analysis of a large amount of data and that appear capable of connecting cyberspace with the physical environment.

It will therefore be necessary to ask whether it is possible to propose a methodology for implementing the supply chain system with blockchain technology to make the sanctioning tools efficient and controllable.

The terms ‘chain of custody' and 'supply chain' couldn't be overlapped even if they are linked.[37]

Specifically referred to the timber sector, the chain of custody certification refers to the generic process of tracking materials from forest to market.[38]

Seeing forest products at every stage of the supply chain, from when the raw material leaves the forest until the final product reaches the consumer, means talking about the supply chain and chain of custody regarding timber.[39] In this sense, the difference between traceability and transparency is relevant. Although they are interconnected and not infrequently used as synonyms, they actually have two different contents. By transparency, we mean the overall visibility of the entire supply chain that allows stakeholders access to the required information without being dispersed, lost, or distorted. In contrast, traceability relates to the ability to access information at a detailed level on everything that remains part of the supply chain; in other words, it can be defined in terms of 'what, how, where, why and when'. The current tracking methods used for the Chain of Custody certification, mainly based on offline analyses, have limitations in dealing with international timber movements and processes linking multiple parties. This

[37] It is possible to define supply chain as the complete life cycle of a product, from its raw material state to its final sale, involving the supply, production, storage, and distribution processes, and requiring coordination between every link in the chain. Instead, the term chain of custody is the chronological documentation that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. It is important to underline that the term ‘chain of custody’ is not limited to the supply chain management, all the while it is crucial in forensics. In the field of criminal evidence, the chain of custody is defined as “the chronological documentation of the movement, location and possession of evidence” (Scientific Working Group on Digital Evidence, glossary <www.swgde.org/glossary>). Even if in different scenarios and with different methodologies, the aim of the chain of custody is the same, that is firstly, to certify that a certain step of a process was conducted following the guidelines and the applicable laws and, secondly, assuring its integrity and the possibility of an *ex-post* revision. See: Giulio Soana, ‘Catena di Custodia, Prova Digitale e Tecnologia Blockchain’ (2021) 4 Diritto di Internet 792.

[38] This analysis wishes to clarify that the complex structure of international timber trading was taken into consideration. However, it was considered impossible to conduct an exhaustive discussion on the comprehensive matter. To give a glance of its structures, it is possible to recall the role of the bill of landing, a transport document issued by a carrier to a shipper covering the carriage of goods by sea. An aspect of interest, in the light of the present analysis is, beyond its structures, the corresponding right of the controlling party. As far as the mentioned right is concerned, the making of a digital bill of landing running on a blockchain could bring together different requirements, e.g., the easy accessibility to data, their transparency and the related tamper-proof. For a more specified analysis, see: Mark L Shope, ‘The Bill of Lading on the Blockchain: An Analysis of its Compatibility with International Rules on Commercial Transactions’ (2021) 22 Minnesota Journal of Law, Science & Technology 163. A different question can be seen within the documentation required by governments for the timber import from non-EU countries as the phytosanitary certificate as well the CITES certificate if the trade regards protected species, see: Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) [2015] OJ L75/4; Regulation of the Commission ‘Implementing Regulation (EU) 2019/2072 of 28 November 2019 establishing uniform conditions for the implementation of Regulation (EU) 2016/2031 of the European Parliament and the Council, as regards protective measures against pests of plants, and repealing Commission Regulation (EC) No 690/2008 and amending Commission Implementing Regulation (EU) 2018/2019’, [2019] OJ L319/1.

[39] Natalia Vidal, Robert Kozak and David Cohen, ‘Chain of custody certification: an assessment of the North American solid wood sector’ (2005) 7 Forest Policy and Economics 345.

makes it difficult to translate into control on a global scale due to several causes, as explained below.[40]

3 Complexity of the timber supply chain: current use of blockchain in the forest sector

Therefore, it is necessary to find a tool that can allow easy traceability from the acquisition of the raw material to the certification of the final product. This need for product tracking in the supply chain is not only an issue in the timber trade but permeates every known production sector and it is addressed differently in many areas. The question arises as to which of the existing technologies would make it possible to store a series of data in an immutable manner and make it searchable even in geographically distant areas and - consequently - the hypothesis of the use of blockchain technology was put forward.

Regarding blockchain, IT infrastructure is now well known in its essentials - although no detailed description and established standards are still lacking - for which a general definition has been adopted from existing blockchain-based systems. [41] Blockchain is an infrastructure characterised by its peculiar structure within the technology of distributed ledger. [42] In very general terms, Distributed Ledger Technology (DLT) refers to electronic ledgers geographically distributed over a vast network of peers. Secure encrypted information storage is based on consensus algorithms involving all or part of the participants. Therefore, when we refer to the blockchain, we refer to an infrastructure in which the ledger is structured as a chain of blocks containing transactions whose validation is entrusted to a consensus mechanism and, therefore, without the need or control of a central authority.[43]

[40] The need to implement timber tracking activities had already been emphasized in 2021 during the 15th Conference of the Parties to the Convention on Biological Diversity and the 26th Session on the United Nations Framework Convention on Climate Change (namely UNFCC), during which the participating nations agreed on actions to mitigate deforestation. The Conference of the Parties is the governing body of the Convention on Biological Diversity, signed in 1992 by 150 government leaders and aimed to promote nature and human well-being. Currently the Convention has 196 Parties (all the countries that have either ratified, acceded to, approved or accepted the Convention are therefore Parties to it). See: The United Nations Framework Convention on Climate Change is an international environmental treaty established to combat dangerous human interference with the climate system, entered into force on 21 March 1994. See: UN Climate Change Conference 'COP26 The Glasgow Climate Pact' (Report, 2021) <https://ukcop26.org/wp-content/uploads/2021/11/COP26-Presidency-Outcomes-The-Climate-Pact.pdf> accessed 29 October 2022.

[41] An appropriate and exhaustive dissertation of the blockchain technology itself cannot be conducted in the present analysis, whereas only the deemed pertinent features are considered.

[42] Following the European Law Institutes' definition, it is possible to affirm that a blockchain is a sub-category of DLT, while blockchains can be defined as "method of operating a distributed ledger. Data are typically stored in blocks organised in an append-only, sequential chain using cryptographic links to validate the integrity of historical data, with algorithmic validation of transaction logic and confirmation of the records by a defined mechanism for consensus among the nodes that process transactions". See: Sjef Van Erp, Martin Hanzl and Juliette Sénéchal, 'ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection' (2022) European Law Institute <www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf>, accessed 18 January 2023.

[43] Each blockchain application has its own rules for validating new data blocks added to the chain, and such validation is based on a consensus mechanism. See: Bahareh Lashkari and Petr Musilek, 'A Comprehensive Review of Blockchain

Why speak of blockchain as a functional IT infrastructure for the supply chain?[44] It is possible to argue that thanks to its own characteristics, a blockchain can fulfil the needs of certainty, transparency and traceability, allowing for full awareness of a product's whole life.[45] Some authors show that blockchain has already been studied and utilised around the timber trade.[46] Blockchain-based applications in forestry are mainly developed (or proposed) in forest management, forest fire detection and traceability of forest-based products.[47] As far as the traceability is concerned, blockchain can be decisive from the moment this technology can validate the lawfulness of the timber sector.[48]

As already mentioned this refers to the use of the blockchain together with tools such as sensors, drones, and even the use of radio frequencies (Radio Frequency IDentification, RFID)[49], capable of guaranteeing the acquisition and collection of data, such as the authorised cutting areas and the collection timing.[50] Two key elements, the morphological characteristics of the materials and the limited technical capabilities, generate a demanding number of challenges and problems for this sector.[51] Exciting studies give a

Consensus Mechanisms' (2021) 9 IEEE Access <https://ieeexplore.ieee.org/abstract/document/9376868>, accessed 8 October 2022; Daniel Minoli and Benedict Occhiogrosso, 'Blockchain mechanisms for IoT security' (2018) 1 Internet of Things 1.

[44] See: Nadia di Paola, *Blockchain e supply chain management. Teoria e pratica manageriale nell'era digitale* (Wolters Kluwer CEDAM, Milano 2018).

[45] For instance, the abovementioned decentralised consensus seems to be a crucial step, seeing as the information of a certain good can be aggregated to something that is accepted by the community—and recorded to the blockchain. See: Lin William Cong and Zhiguo He, 'Blockchain Disruption and Smart Contracts' (2018) National Bureau of Economic Research, Working Paper 24399 <www.nber.org/papers/w24399> accessed 18 January 2023. Moreover, being tamper-proof means that all the data inside of the chain cannot be modified and for this reason the blockchain seems to be suitable as certificate for a raw material as well for the whole supply chain. As mentioned, the FLEGT regulation identify the need of a license scheme for the timber trade; it is at least evocative how the 'FLEGT licence' is defined by article 2(6) of the regulation itself, as "a shipment-based or market participant-based document of a standard format which is to be forgery-resistant, tamper-proof, and verifiable, and which refers to a shipment as being in compliance with the requirements of the FLEGT licensing scheme, duly issued and validated by a partner country's licensing authority. Systems for issuing, recording and communicating licences may be paper-based or based on electronic means, as appropriate".

[46] Zhaoyuan He and Paul Turner, 'Blockchain Applications in Forestry: A Systematic Literature Review' (2022) 12 Applied Sciences <www.mdpi.com/2076-3417/12/8/3723> accessed 29 September 2022.

[47] ibid. The proposed study shows that 52% of the blockchain-based application are related to traceability and it is considered that the best benefits of its use can be qualified in terms of transparency, meaning, in this case, that sellers and buyers of forest-based products can quickly gain access to a variety of necessary information. The product's place of origin, the place of harvesting, the timing of transport, they all information that may minimise the risk of illegal timber being harvested in unauthorised ways or place.

[48] In fact, once the lawfulness of the cut has been proven and the Parties agree on the transport route of this material, any deviation from what is agreed upon is recorded in the blockchain and, as a result, any impermissible variations are rendered impossible (or, if they occur, they can be detected and reported).

[49] The RFID (Radio Frequency Identification) technology automatically identifies information contained in a tag using radio waves. An RFID tag contains an antenna and a microchip to transmit and receive. The mentioned technology is characterized by deploying three essential components: a microchip, an antenna, and a reader. See: Hervé Chabanne, Pascal Urien and Jean-Ferdinand Susini, *RFID and the Internet of Things* (John Wiley & Sons Ltd, 2013) 304.

[50] Carla Smith, 'Blockchain Technology Could Improve Traceability of Wood through the Supply Chain' (2019) 527 Science for Environment Policy: European Commission DG Environment News Alert Service, <https://environment.ec.europa.eu/research-and-innovation/science-environment-policy_en> accessed 23 September 2022.

[51] Margherita Molinaro and Guido Orzes, 'From Forest to Finished Products: The contribution of Industry 4.0 technologies to the wood sector' (2022) 138 Computers in Industry <www.sciencedirect.com/science/article/pii/S016636152200032X> accessed 25 September 2022.

glimpse of the potential use of blockchain in the forest sector, especially about certain aspects of considerable interest, such as preventing deforestation and illegal trade and safeguarding the sustainable forest industry.[52]

One of the first studies on using blockchain technology applied to the timber supply chain dates back to 2018.[53] It pointed out that using a decentralised system makes it possible to exploit the characteristic of non-alterability of data once entered. This allows the creation of a method for certain transactions, even in a rogue ecosystem. Keeping this in mind, it is possible to see the application of blockchain in precisely the two hypotheses we have focused on, namely Russia and Myanmar. A recent study concerning the teak trade from Myanmar has been presented, based on using and implementing a Decentralised Application (DApp) for timber tracking to minimise the gap between physical traders and blockchain, to help them maximise the benefits they can obtain through its use. [54]

The traceability system is, as such, relatively innovative. Still, its particularity focuses on the possibility of tracking the product and its transformation process from the origin to the final stage making it possible to guarantee the accuracy of the input of data, especially in case of its integration with the Internet of Things (IoT)[55] and smart contracts.[56]

A similar study was conducted to verify whether blockchain could prevent illegal bond trading between Russia and China. [57] In this analysis, there is plenty of room to take into

[52] Zhaoyuan He and Paul Turner 'Blockchain Applications in Forestry: A Systematic Literature Review' (2022) 12 Applied Sciences <www.mdpi.com/2076-3417/12/8/3723> accessed 29 September 2022.
[53] Simone Figorilli and others, 'A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain' (2018) 18(9) Sensors <www.mdpi.com/1424-8220/18/9/3133> accessed 10 October 2022.
[54] Studies that have been deemed satisfactory by those who conducted them, although they state that further analysis of this application is needed. The starting point of Sheng and Wicha's investigation relates to the two aspects of product tracking and tracing, where tracking relates to the possibility to know the ongoing location of items during their way through the supply chain, while trancing relates to the ability to know the historical locations, the time spent at each location, record of ownership or farmer, packaging status, processing stages, and warehouse storage conditions for an item. In specific terms, in this case the choice fell on Ethereum. See: Sai Woon Sheng and Santichai Wicha 'The Proposed of a Smart Traceability System for Teak Supply Chain Based on Blockchain Technology' (2021) Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering <https://ieeexplore.ieee.org/document/9425780/> accessed 23 September 2022.
[55] Internet of Things (IoT) is an automated system which allows a universal network of interconnected everyday physical objects which are equipped with uniquely addressable devices, embedded with sensors, software, electronics, actuators to connect and exchange data. See: Srabanti Chakraborty and Prasenjit Das Souvik Pal, 'IoT Foundations and Its Application' in Prasant Kumar Pattnaik and others (eds), *IoT and Analytics for Agriculture* (Studies in Big Data 63 Springer, Singapore 2020).
[56] Justin Sunny, Naveen Undralla and V. Madhusudanan Pillai, 'Supply Chain Transparency through Blockchain-based Traceability: An Overview with Demonstration' (2020) 150, Computers & Industrial Engineering, <www.sciencedirect.com/journal/computers-and-industrial-engineering> accessed 18 October 2022.
[57] It concludes by claiming that this technology, thanks to its innovative features, can solve several problems, especially those related to the transparency of information and the unchangeability of the data entered. Therefore, this study believes that blockchain has the potential to be a viable solution to implement and improve upon current approaches. See: A Vilkov and G Tian, 'Blockchain as a Solution to the Problem of Illegal Timber Trade between Russia and China: SWOT Analysis' (2019) 21 International Forestry Review <www.ingentaconnect.com/content/cfa/ifr> accessed 23 September 2022.

account the sector's peculiarities, especially at the level closest to harvesting areas, which suffers from a lack technological infrastructure.[58] Consequently, it is necessary to stress that in the forest sector the use of blockchain technology is a reality that - although not yet widespread - appears to be of exemplary implementation.

Even before we can speak about their dissemination, certain aspects must be carefully analysed and regulated. We must consider how to ensure data entered into the blockchain is genuine, as well as how to protect it and guarantee accuracy in algorithm creation. This will provide tools for resolving conflicts that may arise. The mutual recognition of certificates is one facet of building a complex plan.[59] The advantage of using blockchain to issue certificates of origin would be "limited" to the integrity of the accompanying document of the goods, thus providing proof that they have not been manipulated.

The above relates to the so-called oracles, i.e., all those systems that enable data entry on the blockchain and thus represent the point of contact between the off-chain and on-chain worlds (and vice versa when exporting previously entered data).[60]

However, suppose it was possible to implement the use of this technology to rely on the data entered and stored on the blockchain without thus relying on off-chain certification and control authorities. In this case, there could be more than one benefit, such as reducing customs costs, reducing the risk of fraudulent activities, and increasing the accountability of the supply chain.

The above is easier to realise as far as technology is possible; this issue is obviously not undermined by the European institutions, which design the 'Forest MAP' as a framework within which all new policies concerning the forest sector must be considered.[61]

Eight priority areas have been identified to cover the three pillars of sustainable forest management, which are social, economic, and environmental. For example, those operating in rural and mountain areas in Italy have pointed out how the emergence of technical and economic barriers poses a real risk to the exclusion from the system of small

[58] I.e. we can mention a project established in Brazil and which aims to ensure transparent trade transactions of legal and sustainable forest products that meet the requirements of the EUTR and the Lacey Act. See: BVRio's Responsible Timber Exchange Trading Platform <www.bvrio.com/plataforma/plataforma/madeira.do?language=en-us>.

[59] Jule Giegling 'In Blockchain We Trust? Certificates of Origin as a Case for Distributed Ledger Technologies' (2022) 1 Journal of Law, Market & Innovation 70.

[60] Systems that, can be hardware, and software, but also human in nature, depending on the origin of the data and information transferred. Looking for a brief and not exhaustive exemplification, in the case of a hardware oracle, the data is created in the physical world (the geolocation of a cut) and is detected by technological tools such as GPS. In the case of software oracles, the data are native online, i.e., they are created in the digital world, like data traffic generated by an IP address. Lastly, there is the possibility of human oracles, that enter data, which, can also be the result of the evaluation or interpretation of data generated by software or hardware. See: Laura Vagni, 'Il Problema della Rilevanza Giuridica dell'errore nella Decisione dell'oracolo della Blockchain' (2022) 2 lceonline <www.lceonline.eu/blog/2022/06/28/il-problema-della-rilevanza-giuridica-dellerrore-nella-decisione-delloracolo-della-blockchain> accessed 3 November 2022.

[61] Eight areas of action were pinpointed: 1) supporting our rural and urban communities; (2) promoting the competitiveness and sustainability of forestry, bioenergy, and green economy industries in general; 3) forests in a changing climate; (4) protecting forests and improving ecosystem services; (5) information and monitoring of forests; (6) research and innovation; 7) working together; and 8) forests from a global perspective. See: European Parliament 'The European Union and Forests' (Fact Sheets on the European Union) <www.europarl.europa.eu/factsheets/en> accessed 10 November 2022.

and medium-sized enterprises struggling to integrate digital technologies into their activities.[62] It is clear that these problems, if already present in some areas of Italy, are even more penetrating in other areas of the globe, contributing to the widening of the already existing digital gap. The question remains, therefore, whether blockchain has the necessary features to be used in specific contexts, either to enable or prevent certain actions, or as a tool to verify the product's chain of custody and perhaps directly apply the penalty or reward regime.

The matter about is of the utmost importance because if what the EIA stated in its report titled 'the Italian job' is correct, it is certainly relevant to know that a company that imports in violation of the EUTR can simultaneously continue to benefit from EU development funding.[63]

Another recent study argues that the movement of European funds via a platform that exploits the blockchain plan would achieve three types of benefits: traceability of flows, accessibility of data, and isolation of malicious actors.[64]

In the hypothesis of the timber supply chain, transparency in the chain of custody from the marked timber, from the landing site and up to the finished product would not only create a supply chain of the knowledgeable actor. Still, it would also be able to exclude the financing of non-compliant Parties.[65]

For instance, producers, forestry companies or importers and processors who choose a transparent and verifiable supply chain could be recognised as performing parties.

[62] See: Stefano Ciliberti and others, 'Digitalizzazione e Tracciabilità: I Principali Risultati Del Living Lab Sulla Filiera Legno-Energia in Italia' (2021) 18 Forest@ - Journal of Silviculture and Forest Ecology 79 <https://foresta.sisef.org/contents/?id=efor3982-018> accesses 17 November 2022; Piermaria Corona, Gianfranco Scrinzi 'Security of the Wood Production from the Italian Forests and Innovation for Wood Product Traceability' (Atti del Secondo Congresso Internazionale di Selvicoltura dell'Accademia Italiana di Scienze Forestali, 2015) <https://aisf.it/2cis-pc-sic/> accessed 18 October 2022.

[63] Environmental Investigation Agency, 'The Italian Job How Myanmar timber is trafficked through Italy to the rest of Europe despite EU laws' (2021) <https://eia-international.org/wp-content/uploads/The-Italian-Job-2021-SPREADS.pdf> accessed 14 October 2022.

[64] The fairness of the disbursement and distribution of European funds has always been the subject of careful analysis reinforced following the Covid-19 pandemic that saw numerous economic resources deployed by the European Union to try to stem the devastating consequences brought about by the pandemic emergency. The current problem of the proper allocation of funds, which must be conducted in such a way that they can be received by the Parties legitimately entitled to use them, and which finds elements of serious criticality in the transnational dimension of the transactions and the absence of a central investigative body in the Member States. Following this reflection, according to the writer's opinion, implementing the use of blockchain technology in strategic and specific areas would delineate a new virtuous model, also capable of providing a correction to situations, such as those under consideration, pertaining to compliance with the sanctions imposed, as well as all regulations. See: Marco Letizi, Giulio Soana 'Blockchain e Intelligenza Artificiale a fini Antifrode: Il Caso dei Fondi Europei' (2020) NT+ Diritto <https://ntplusdiritto.ilsole24ore.com/art/blockchain-e-intelligenza-artificiale-fini-antifrode-caso-fondi-europei-ADLd4h7> accessed 14 October 2022.

[65] With specific reference to the teak trade, which sees the ban of exporting entities that have relations with the military regime established in Myanmar, being able to see the country and place of origin (understood as the territory where the timber is felled) in detail, would allow producers who are not affected by the sanctions to be chosen, thus allowing only them to continue their trade flow with foreign countries. Concerning Myanmar, the question is about the distinction between legal and illegal importation depending on who is involved. For what comes from Russia and Belarus, it is necessary to stop the materials at the border and check that the timber has not been moved and processed in other states. Once Russian timber has entered the European market, it is difficult - if not impossible - to distinguish it from wood from other areas, so only with complete traceability can its legality be guaranteed.

Accordingly, blockchain can be seen as a 'certification of merit' that would allow even a small company to participate more easily in calls for tenders.

4 Prospects and concluding remarks

These issues are already a priority for institutions that have begun questioning their possibilities for future development. [66]

The above underlines how the attention of authorities is shifting towards the search for increasingly effective tools, a need that arises from the complexity and mutability of markets and circumstances that have already been extensively marked. We can more generally state that, focusing on the movement of goods, it is possible to identify their passage across borders between States as a control gate. As far as the European Union is concerned, compliance with the regulations of the sector under analysis is guaranteed in the first instance by the customs authorities of the Member States as the competent Bodies to implement the so-called import control.[67] A further matter is the legal relevance of interference by a subject outside of sovereignty governs; the perspective must focus on the topics that are legitimately addressed following the rules.[68] Moreover, another aspect

[66] Some projects of interest relate specifically to certificates of origin, for which the European Commission is questioning how to implement the necessary documentation for the cross-border movement of goods, considering that distributed ledger technologies such as blockchain can support certification and verification procedures for the origin of products. Among the novelties worth mentioning is the DPP (Digital Product Passport), which will see its application - as of 2024 – and described by the European Parliament in the following terms: "a digital document that provides updated product information through the value chain and product life (origin, composition, repair and disposing of)" and for which the European institutions are currently evaluating the pros and cons of its use both on-chain and off-chain. Created specifically with the manufacturing sector and the protection of 'made in' in mind, it is nevertheless a tool that will have to be viewed carefully once the two operating methods have been fine-tuned, whether it can be proposed in different sectors and with partially or different purposes. See: World Customs Organisation, 'Comparative Study on Certification of Origin' <www.wcoomd.org/-/media/wco/public/global/pdf/topics/origin/instruments-and-tools/comparative-study/related-documents/comparative-study-on-certification-of-origin_2020.pdf?db=web> accessed 01 November 2022; European Parliament, 'New technologies and new digital solutions for improved safety of products on the internal market (Study Requested by the IMCO committee), <www.europarl.europa.eu/RegData/etudes/STUD/2022/703348/IPOL_STU(2022)703348_EN.pdf> accessed 2 November 2022.

[67] At this stage, the possible risks are identifiable in several respects. The possibility of circumventing bans in the case of imports from countries that have not joined the sanctions package appears particularly relevant. The easiest method of circumventing sanctions to date is timber trade with countries with no restrictions on trade relations with sanctioned countries, as analysed by the EIA. Given that different practices and laws may be appropriate in individual Member States, it is not out of the question that goods legally permissible for entry could be blocked due to irregularities, even purely formal ones, in the transport documents. This is because we are dealing with international trade.

[68] In the case of the sanctions on Russia, Belarus and Myanmar, the latter did not accept the restrictions imposed, which, of course, were issued unilaterally; therefore, for the sanctioned States, existing relationships (and future ones if created) would continue to be by the National Law. The observance or implementation of sanctions imposed between States cannot fail to come up against issues about the theory of Law, with the intention of understanding whether - and how - authorities external to one or more government can impose themselves in business relationships, between Parties that have not previously adhered to a specific regulation in this sense. For instance, the Belarusian exporter cannot have a contract legitimately concluded before the sanctions were enacted and cancelled by an entity - such as an EU institution - that has no authority over it: the timber imported by the European Union trader becomes illegal because it is contrary to European Union law, while remaining legal for the producer in the country of origin and for all countries that have not implemented the sanctions, and this timber is transported along more or less defined trade routes, which may make it confusing or impossible to sanction even within the European Union itself. Consequently, once the end-

that needs to be considered is how disputes can arise, not only in proposed cases, where a party has to interrupt the execution of a contract due to the introduction of a new regulation, but also in other cases: where a smart contract transaction is not completed, or is only partially completed, or is not entered into the blockchain. In the situations mentioned questions arise concerning the imputation of liability.[69]

Even if the data in the mass memories of each node are physically traceable - at least partially – but fundamentally decentralised, could we assume that the competence for resolving such issues is equally decentralised?[70] Some authors are proposing an alternative approach to the existing exercise of jurisdiction, an approach inherent to blockchain technology itself and responding to the term distributed jurisdiction, which would, in any case, require a governance system within the blockchain technology itself; hence all the difficulties and questions to which it is still not possible to offer an answer to date, as outlined below.[71] Reversing the perspective, we see no interference and control of the blockchain by an authority but a system that allows the chain of custody to be demonstrated.[72] Therefore, a suitable structure should be created for a certified on-chain, for which it is crucial that the underlying institutional framework can provide legal recognition of the information generated therein to enable its use on the market.[73]

The above is part of a context that is still full of questions and requires extensive research and research, whose extent is undoubtedly so broad that it does not allow a thorough comment on state of the art in this paper.[74] In conclusion, using the blockchain

user receives a consignment of timber, or the consumer, the question of its provenance may involve several off-chain entities, ranging from public administration - as Customs authorities and others - to the producer, as well as the transport companies used, but also partly on-chain, such as the validator node of individual transactions, as well as the company developing the apps used, or the technologies used for data collection.

[69] A further issue arises from the fact that, since we are inside a computer system, the questions of who owns the network and its data take work to resolve. See: Adam P Balcerzak and others 'Blockchain Technology and Smart Contracts in Decentralized Governance Systems' (2022) 12(3) Administrative Science <www.mdpi.com/2076-3387/12/3> accessed 31 October 2022.

[70] Matters such as who is responsible for, who has processed what data, where and when, and thus ascertain which jurisdiction should apply in disputes, or who controls the information and is responsible for its security or responsible for its integrity. See: European Union Blockchain Observatory & Forum 'Legal and regulatory framework of blockchains and smart contracts' (Thematic Report 27 September 2019) <www.eublockchainforum.eu> accessed 30 October 2022.

[71] Bronwyn E Howell and Petrus H Potgieter, 'Uncertainty and Dispute Resolution for Blockchain and Smart Contract Institutions' (2021) 17(4) Journal of Institutional Economics <www.cambridge.org/core/journals/journal-of-institutional-economics/article/abs/uncertainty-and-dispute-resolution-for-blockchain-and-smart-contract-institutions/6C06720B46228EA9D95E5E7611E5EFA5> accessed 06 June 2022; Yann Aouidef, Federico Aste and Bruno Deffains, 'Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects' (16 March 2021) Frontiers <www.frontiersin.org/articles/10.3389/fbloc.2021.564551/full> accessed 06 June 2022.

[72] For example, the execution of a contract in violation of the applicable regulations would have several consequences that would no longer make it convenient to act this way.

[73] It is difficult, at this point, not to think about the possibility that Decentralised Autonomous Organizations (DAOs) could form the parties involved. Decentralised Autonomous Organisations are blockchain-based entities that allow their members to coordinate and regulate themselves via a set of self-executing rules, implemented on a public platform and with decentralized governance. See: Samer Hassan and Primavera De Filippi, 'Decentralized Autonomous Organization' [2021] Internet Policy Review <https://policyreview.info/glossary/DAO> accessed 5 November 2022.

[74] It is possible, however, to mention how among the issues that still awaiting a resolution is the current question of blockchain governance, a terminology that is used in two heterogeneous contexts, namely governance within the blockchain and governance with the use of the blockchain. As for the interest in the present analysis, reference can be

to control and implement sanctioning regimes imposed between communities certainly appears to be a tool of unquestionable usefulness, not only broadly speaking but also referring - as seen - to a specific production sector affected by the enactment of trade restrictions.

Regarding the numerous issues from this analysis, it is equally undeniable that several entities need joint action to become a regulatory landscape that can effectively enable its use.

Although some sanctions have been effective for some time, it is not unwise to assume that it is only in the current events of the Russian-Ukrainian conflict that global awareness has increased to the point of trying to make the restrictions imposed effectively. It will therefore be necessary to see how the authorities of the various countries move to fulfil their commitments and, therefore, analyse how the - possible - violations detected can be stemmed with the use of blockchain technology.

made to what Fischer and Valiente state: "in a broad sense, blockchain governance can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organization. Importantly it refers to the entirety of motivations, rules, and activities that feed into the establishment of choices and subsequently deciding on them, and includes, but is not limited to, any coded on-chain rules that guide these processes". See: Aaron Fischer and Maria-Cruz Valiente, 'Blockchain Governance' (2021) (10) 2 Internet Policy Review <https://policyreview.info/glossary/blockchain-governance> accessed 14 November 2022.

*Olesia Shmarakova**

SANCTIONS, OPEN-SOURCE SOFTWARE, AND OPPOSING TRENDS IN SOVEREIGNTY

Abstract

Sanctions have long been part of the international relations between States; they are used by different States and affect different areas. Among the different types of sanctions, sanctions relating to technology and innovation are of particular interest because they are likely to have the most long-lasting effects.

Today, despite the fact software development issues are not as topical in academic literature as cryptocurrencies or non-fungible tokens (NFTs) are, there is no denying that software development and licensing plays a significant role in the economy. Software exists at the heart of all emerging technologies, and a large part of a technology's success depends on its quality and efficiency. A peculiarity of software development is the phenomenon of open-source software - code made publicly available by the developer to the entire community. It is difficult to imagine modern software development without the use of open-source.

This article aims to analyse the applicability of economic sanctions to open-source software given its international character and peculiar distribution model.

The first section will describe the phenomenon of open-source software as such, its key characteristics, and distinguishing features that are relevant for the application or non-application of sanctions rules. It will also address the problem of defining jurisdiction over open-source software, taking into consideration the international dimension of cyberspace, which leads to a discussion about the erosion of State sovereignty along with the other emerging technologies.

The second section will cover US and EU sanctions relating to technology and innovation, primarily with regard to software. The design of sanctions will be compared and the key distinction concerning the extraterritoriality of sanctions will be discussed.

In the third section, specific provisions of sanctions regulations will be applied to free and open-source software (FOSS). In particular, the five-step model for determining the applicability of US export control regulations to FOSS will be described. The specific US approaches to determining jurisdiction based on the presence of US components in a product will be discussed. Thereon, a new model for determining jurisdiction specifically in the area of technology and innovation will be discussed, which goes beyond the usual territorial and national principles and constitutes a new legal basis for the extraterritorial application of the law.

Finally, the last part will contrapose the two trends described above: first, the erosion of sovereignty due to the development of new technologies, and, second, the reassertion of sovereignty as the State begins to legislate in the areas previously free from regulation and to apply new approaches to the definition of its jurisdiction.

JEL CLASSIFICATION: F51; H73; K24; K33; L17; L86; O30

* Postgraduate student at University of Turin, European Legal Studies.

SUMMARY

1 Introduction

Sanctions have long been part of the international relations between States; they are used by different States and affect different areas, from restrictive measures on particular individuals and companies to economic sanctions, from diplomatic sanctions to bans on media.

Issues relating to innovations and technology are covered by economic sanctions, which generally target specific economic sectors, but may also have a general impact on the ability of the sanctioned country to carry out its unwanted activities. In this latter case, the sanctions in the aggregate impact on economic status and technological progress of the sanctioned country, stripping it of financial resources and/or the possibility to improve technologically.[1]

Sanctions targeting technology and innovation are of particular interest for two reasons. On the one hand, they may have the most significant effect in the long term to guarantee the technological inferiority of the sanctioned State. On the other hand, to be enforceable and effective, such legislative measures must be in line with the essence of technological innovation and take specific characteristics into account, which often requires the application of new legislative methods.

The most important examples in the global practice of technology and innovation sanctions are the US and the EU sanctions, and their approaches to the wording, degree of technical detail, and general policy differ significantly.

Given the role that software development and licensing play in today's world, unsurprisingly, both US and EU sanctions apply to this area as well. And it is difficult to imagine modern software development without the application of the already existing tools, primarily so-called open-source software – the software with open-source code freely available on the Internet. Open-source software is developed by the international

[1] For example, as the European Commission explains in its with regard to the issue of sanctions affecting ordinary people, sanctions against Russia *"aim at weakening the Russian government's ability to finance its war of aggression against Ukraine* […] *sanctions are designed to maximize the negative impact on the Russia's economy*", see 'Consolidated FAQs on the implementation of Council Regulation 833/2014 and Council Regulation 269/2014 (2022)', para A 1. 6 <https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en> accessed 20 March 2023.

IT community and distributed free of charge to anyone who wants to use it based on unilateral licenses.

It is a common belief that economic sanctions do not apply to open-source software.[2] As with many common beliefs, this is true, but not the whole truth. Moreover, it should not be forgotten that the phenomenon of open-source software is just one example of modern technical innovations, and as such, follows the general de-regulation trend.

This paper will analyse US and EU software-specific sanctions and their application to open-source software in particular. It should be noted that this article will predominantly use the sanctions imposed against the Russian Federation as an example, since they are broad and represent latest practices. The technological peculiarities of open-source software will also be touched upon in order to evaluate whether and how effectively they are addressed by sanctions legislation, and whether there are any new trends in sanctions regulation in general.

2 FOSS specifics

2.1 What is FOSS?

Free or open-source software is not a new phenomenon as such. The literature on it is vast, both in the legal and IT spheres. For this reason, this paper will only briefly cover the main features of open-source software with a focus on issues that are relevant to the application of sanctions.

So-called free software originates from US academic circles, which started to question the restrictive nature of exclusive rights under intellectual property laws. Richard Stallman, an ex-MIT academic is the free software pioneer who founded the Free Software Foundation (FSF) in 1985, and which still exists today.[3]

The FSF approach is explained by the four freedoms of what a user can do: to run, edit, contribute to, and share the software. At that stage, it was out of the question if free software is to be “free-of-charge” or not; Stallman himself stressed that it is as “free as free speech, not as free beer”.

A bit later, another association arose, the Open-source Initiative, which has developed ten criteria to determine whether a license for software is open-source.[4] One of the important criteria is the distribution of the software without any royalty or fee.[5] For the

[2] The Linux Foundation which is usually concise in its communications, since it addresses the IT community and not the lawyers, released a 15-paged long report explaining how USA sanctions do not apply to the open-source technologies, see Steve Winslow and others, ‘Understanding Open-source Technology & US Export Controls’ <www.linuxfoundation.org/resources/publications/understanding-us-export-controls-with-open-source-projects> accessed 17 February 2023.
[3] Free Software Foundation <www.fsf.org> accessed 20 February 2023.
[4] The Open-Source Definition <opensource.org/osd> accessed 20 February 2023.
[5] Of course, at the stage of its appearance and sometime after FOSS drew criticism from commercial IT corporations that sold software licences for money. FOSS advocates were seen as almost hackers. Bill Gates, in particular, called

present paper, other criteria are also important: free redistribution, non-discrimination of persons or groups, and non-discrimination in fields of endeavour (for example, limiting use to non-commercial purposes is not permitted).

The Open-source Initiative, among other things, validates the standard licences for eligibility to the said criteria, and there is already a significant quantity of licences on their list. All the most popular types of licences are open-source licences. Still, this does not prohibit developers from the possibility to use any other existing licence or even drawing a new licence of their own.

Therefore, free software and open-source software are not the same thing, although they are quite similar. One piece of software which is distributed via the Internet in a form of a source code may fall under both sets of criteria or only one of them, depending on the details. However, for this paper the possible differences do not matter, therefore we will address all such software under one term "FOSS" (free/open-source software).

The most important characteristic of FOSS is the licence. Contrary to popular belief, FOSS is still protected by intellectual property law and is not in the public domain. The licence published together with the source code sets out the obligations and the restrictions for the user. FOSS licences are numerous, though there is a set of standards, popular types of licences – namely those approved by the Open-source Initiative. It is important to mention that the licence usually covers only rights and restrictions for the user; defining an applicable law or competent court is a very rare thing. Generally, the standard licences are worded in a way to be used without alteration by any developer from any State, depending on their approach to the set of rights provided to the user. So, for example, to publish the software under the MIT licence one does not have to have any connection to the Massachusetts Institute of Technology (MIT).

In practice (although it is not stipulated in any official way) three groups of FOSS licences are distinguished: permissive, weak copyleft, and copyleft. Permissive licences do not impose usually any restrictions on the disposal of the modified products based on FOSS and only require the initial author's copyright to be kept (MIT and Apache are typical examples). Weak copyleft requires that the source code of the modified work is made publicly available under the same licence, however, the publication requirement does not cover any other code used in the final product (this type of licence is usually applied to software libraries). And finally, copyleft is a type of licence requiring licensing of a whole new software under the same licence (different versions of GNU General Public License (GPL) are perfect examples here). The important issue is that some types of FOSS licences set restrictions and requirements relating to the further use of software, which is unfeasible for the public domain.

them "modern communists", see Scot Colford, 'Explaining Free and Open-Source Software' (2009) 35(2) Bulletin of the American Society for Information Science and Technology 10.

Despite the initial criticisms of FOSS, it became more and more popular. Nowadays one can hardly find a software product where no FOSS has been used. Individual developers as well as big commercial corporations contribute to the creation of FOSS. Moreover, one of the main advantages of FOSS for any type of user is that popular FOSS is continuously evolving in the community. There is a whole ecosystem of FOSS developers and users who constantly improve the code, find bugs, and add new features. Therefore generally popular FOSS products enjoy high-quality code since it is reviewed by the community.[6]

One of the main characteristics of FOSS is that it is not just software with a publicly available source code, but a living community of developers from all over the world. The creation of a single FOSS may be a result of contributions by many programmers of different nationalities, sometimes using nicknames at huge aggregator sites like GitHub. This makes the FOSS community an integral part of cyberspace as an international community beyond State borders and largely beyond the reach of the State.

2.2 Problems of jurisdiction over FOSS: contribution to sovereignty erosion

FOSS as a phenomenon poses some legal challenges for practitioners. First of all, there is a copyright issue: from the start, FOSS presupposes the possibility of its use and modification by any user, meanwhile, a "classic" copyright would require an author's consent in each case (to say nothing about the moral rights of the author). To stress this difference the very name "copyleft" was introduced as a licence type to distinguish FOSS.

Such purely private law issues are not the only challenges created by FOSS. With "classic" copyright, there are usually no difficulties in determining the applicable law or court jurisdiction. As a rule, it would be the law of the country of the author or other intellectual property owner[7], unless the parties have specifically agreed otherwise. But defining the law applicable to FOSS may be quite difficult because of the following:

First, there is no indication of applicable law in the text of the license. It should be noted that no standard license contains such a provision because of the focus on universality and workability for developers from any State. In some cases though, developers may add applicable law clauses to the standard licence text; because of that, the indication of the standard licence type should not preclude the need for lawyers to read it carefully.

In addition, it is not always clear who is the owner or developer of a particular FOSS and what national law therefore applies to them. In cases where it is a corporation, no problems will arise, but with an individual, the answer may be not evident. Moreover, it is still a widespread practice that developers whom you would meet at the sites like GitHub use pseudonyms.

[6] Mark Henley and Richard Kemp, 'Open-source Software: An introduction' (2008) 24 Computer Law & Security Report 77.
[7] Mireille van Eechoud, *Choice of Law in Copyright and Related Rights* (Kluwer Law International 2003) 179.

And finally, there may be many individual developers and contributors from different States, so private international law rules are of no help. There is usually no agreement between them on any such thing as the law applicable to their FOSS.

Similarly, it may be unclear which court would be competent to deal with FOSS-related disputes. For example, if a developer publishes their FOSS under a copyleft licence, like GPL v.3, and the user from another country creates a proprietary software on this basis and sells it without disclosing the code, the developer may face a problem in defining the competent court. Disputes of this type exist, though it should be admitted that their quantity is negligible compared to the widespread use of FOSS – which is also an important characteristic of the FOSS phenomenon.[8]

In general, in the IT community – excluding large commercial corporations – it is rather uncommon for disputes to be resolved in court. It is even more uncommon for the FOSS community since FOSS development is in itself a non-commercial activity. One can say that FOSS has value but does not have a price. FOSS is a community based on trust, and reputation is extremely important. Therefore, both developers and users of FOSS generally follow established community practices in good faith even in the absence of legal certainty.

Moreover, the FOSS community as a whole is more tolerant rather than welcoming when it comes to any type of legalese. Whoever wants to defend their rights rigorously using legal methods does not usually engage in FOSS development. It is technically very difficult to monitor all possible violations. Of course, there are standard licences that impose quite a lot of requirements to respect the author's rights (in fact, all copyleft ones). But it is hard to imagine that the author of the "beerware licence"[9] or the "chicken dance licence"[10] would sue the infringer even if they succeed in collecting sufficient proof of the violation.

Having regard to the above, it may be contended that the FOSS community strives to be free from any jurisdiction, and this is more a characteristic of the specifics of the FOSS phenomenon as such rather than a conscious legal position.

Both individual and corporate FOSS developers are indeed nationals of some States, however, this is in itself rather a challenge to FOSS development than the other way around. In some cases where FOSS is published by corporations, it may be presumed without additional analysis that the law of the State of registration of the developer would

[8] Notwithstanding the time passed, for ordinary commercial disputes, it is still possible to agree with litigation risk evaluation given by Lawrence Rosen, a past General Counsel of the Open Software Initiative: "The risks are law": Lawrence Rosen, *Open-source Licensing, Software Freedom and Intellectual Property Law* (Prentice Hall, 2004) 269. The basis for this conclusion lies at the very heart of the licensor-licensee relationship, which has not changed with time. The same is noted in the subsequent works, eg Henley, Kemp (n 6).

[9] Beerware Licence <https://gist.github.com/azizshamim/660282> accessed 13 February 2023.

[10] Chicken Dance Licence <https://github.com/supertunaman/cdl> accessed 13 February 2023.

be applicable. An example of such FOSS may be the Hyperledger blockchain based on contributions from IBM and Intel[11] or Red Hat software.[12]

It is clear that since FOSS has become so important and valuable to modern software development the most powerful States may pursue FOSS regulation to the extent allowed by international law. And this is where the problems described above concerning the definition of the State's jurisdiction over particular FOSS items arise.

For these reasons, FOSS is often (and justifiably) regarded as independent software positioned beyond the jurisdiction of any State and, to a lesser extent, beyond any political influence.

The FOSS community seems too large and too heterogeneous; a few big corporations involved in artificial intelligence development (as it usually requires significant investments) may be controlled. But trying to control millions of individual developers worldwide who jointly contribute to FOSS projects, use pseudonyms, and generally know more about IT than any government official may be totally in vain.

In addition, the openness of FOSS, like Wikipedia, creates advantages for all from basic users to corporations and to the State itself. The FOSS community cannot be divided between the most powerful States like the Antarctic.

For the reasons outlined above FOSS is frequently regarded as an ideal alternative for States wishing to increase the level of digitalization without becoming economically and politically dependent on the States producing proprietary software. FOSS is repeatedly being called a vehicle to achieve digital and technological sovereignty.[13]

However, the question is how exactly we define sovereignty. The above examples are more about technological and digital independence, and the main question is – independence from whom or what? The reply in the case of software is evident, as the US holds a significant share of the world market, and majority of the "mass-market" software (like office programs or operational systems) is of US origin.

It is questionable whether we can talk about more internal sovereignty due to the mass use of FOSS by the State. If sovereignty is evaluated in terms of effective control, FOSS by its very nature does not provide more control to anyone – neither to the State of origin

[11] Hyperledger Foundation <www.hyperledger.org> accessed 14 February 2023.
[12] Red Hat 'Our code is open' <www.redhat.com/en/our-code-is-open> accessed 15 February 2023.
[13] Besides the sanctions issues, FOSS advantages are often emphasized in the context of digital independence of the states, in particular, as a way to avoid the obligation to comply with intellectual property rights and to pay the royalties for the software originating from the dominating states and by doing so contribute to their dominance. See European Commission, Directorate-General for Communications Networks, Content and Technology, Knut Blind, Sivan Pätsch, Sachiko Muto and others 'The impact of open-source software and hardware on technological independence, competitiveness and innovation in the EU economy: final study report' (Publications Office, 2021) <https://data.europa.eu/doi/10.2759/430161> accessed 20 March 2023. See also Ian Cook and Gavin Horobin, 'Implementing eGovernment without promoting dependence: open-source software in developing countries in Southeast Asia' (2006) 26(4) Public administration and development 279; Alireza Amrollahi, Mohammad Khansari and Amir Manian, 'Success of Open-source in Developing Countries: The Case of Iran' (2014) 5(1) International Journal of Open-source Software and Processes 50.

nor to any other State. Therefore, it can be contended that using FOSS will instead lead to technological neutrality and independence than to sovereignty in the traditional sense.

It is popular discourse nowadays that emerging technologies, such as the Internet, Bid Data, and cryptocurrency contribute to the erosion of State sovereignty[14], since, due to their technical features, they extend beyond traditional territorial boundaries and exist only in cyberspace. Legislative regulation as well as effective control by the State is hampered by the technical essence (for example, inherently high levels of anonymity in blockchain or decentralized cryptocurrencies[15]). One can agree with the statement that "the notion of territoriality is challenging in cyberspace. The essence of activities in cyberspace is within the virtual dimension, i.e., the data and the virtual personae are not connected to the territory of a State".[16]

FOSS can hardly be called an "emerging technology"; indeed, it is not a unique technology at all but rather a framework for software development. The technical side of programming has not changed much over the years. However, in practice, it turns out that the cooperation framework which constitutes the very basis of FOSS may be no less important than the technical aspects.

Therefore, we can rightfully speak of jurisdiction and even sovereignty (as the practical embodiment of a legal right to control, together with the technical possibility of effective control) not only in relation to emerging technologies like blockchain, artificial intelligence, and Big Data, which are discussed widely but also with regard to FOSS.

As a matter of fact, States have little control over the usage of FOSS compared to the classic proprietary licensed software. In the case of a classic licence, the State may execute different control procedures over the business and request the licence contracts, for example, within the tax compliance check. But there is nothing to request for FOSS. Moreover, while FOSS is distributed free of charge, similar free proprietary licence contracts, depending on the jurisdiction, may create additional difficulties: for example, the law may prohibit a commercial company from receiving any free-of-charge services or goods[17] or may require payment of additional taxes. With respect to FOSS these and other legal aspects stay totally out of governmental control.

[14] See, for example, David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367; Henry H Perritt Jr, 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance' (1998) 5(2) Indiana Journal of Global Legal Studies 423; Gerald Kreijen and others, *State, Sovereignty, and International Governance* (Oxford University Press 2002); Martin Loughlin, 'The erosion of sovereignty' (2016) 2 Netherlands Journal of Legal Philosophy 57; James A Lewis, 'Sovereignty and the Evolution of Internet Ideology' 2020 <www.csis.org/analysis/sovereignty-and-evolution-internet-ideology> accessed 19 February 2023.

[15] Douglas W Arner and others, 'Ukraine, Sanctions and Central Bank Digital Currencies: The Weaponization of Digital Finance and the End of Global Monetary Hegemony?' (2023) 7 Asiaglobal Papers <https://ssrn.com/abstract=4133531> accessed 18 February 2023.

[16] Peter Pijpers and Bart van den Bosch, 'The "Virtual Eichmann": on sovereignty in cyberspace' (2020) Amsterdam Law School Research Paper 65/2020 Amsterdam Center for International Law 33/2020 <https://ssrn.com/abstract=3746843> accessed 15 February 2023.

[17] Eg, art 575 of the Russian Civil Code expressly prohibits gift-giving between commercial entities.

The contribution of FOSS to the "erosion of sovereignty" is not discussed widely in academia, compared to discussions over cryptocurrencies (financial flows going beyond the control of central banks), the Internet as such (loss of State control over the information flows) and Big Data (State losing its data monopoly). The phenomena of cyberspace pose a threat to the status quo and the level of State control over the relevant sectors in previous periods. As for FOSS, one can hardly acknowledge that it poses any significant threats, which may be the reason for the lack of academic attention.

However, if we look at the essence of these phenomena, we see similarities in all of them: existence in cyberspace, high levels of distribution, the prominent role of individuals, technically embedded anonymity, and the existence of an international professional community.

States, in general, do not seem to be particularly concerned about FOSS until they try to control and regulate it (which most States have not been doing previously, in contrast to the financial system, which was always a highly-regulated sphere). What would encourage States to be concerned with the regulation of the FOSS? First of all, it may be the sanctions relating to technologies and software, and effective regulation would be important for both sides – the State imposing the sanctions and the State trying to circumvent them or minimise the negative consequences.

As for the erosion of sovereignty by the very existence of FOSS and similar phenomena, there is no denying that some States do not ignore it and try to counter it. For example, Russia is creating a governmental FOSS register to provide licences to State-owned FOSS (for now as an experiment).[18] Considering the political circumstances not limited to official sanctions of the other States but also to the position of the private actors[19] and risks of malware FOSS distribution[20], it seems to be a reasonable step. Of course, such an approach does not solve the problem that the quality of FOSS is linked to the community involved in its improvement, and the wider the community, the better it is.

Moreover, in Russia besides the general procedure of software depositing with the patent authority, there is another optional registration procedure relating to proving the Russian origin of software with the Ministry of Digital Development, Communications and Mass Media[21], which is obligatory for participation in State procurement and receiving some tax benefits. And for this particular registration some types of FOSS, primarily under copyleft licenses, may be a "red flag". In this manner, the State seeks to gain at least some degree of control over the FOSS sphere.

[18] Regulation of the Government of the Russian Federation 1804 of 10 October 2022.
[19] See, for example, the discussion of the GitHub approach to sanctions below.
[20] Raula Gaikovina Kula and Christoph Treude, 'In War and Peace: The Impact of World Politics on Software Ecosystems' (2022)<www.researchgate.net/publication/362429395_In_War_and_Peace_The_Impact_of_World_Politics_on_Software_Ecosystems> accessed 15 February 2023.
[21] See Registry of the Russian Software <https://reestr.digital.gov.ru> accessed 20 February 2023.

In summary, one cannot deny FOSS contribute to the erosion of the State sovereignty, as de facto whole sets of transactions related to the development, distribution, and use of FOSS is beyond the sphere of the State's control.

3 Economic sanctions in the areas of technology and software: comparison of EU and US approaches

This section will cover issues relating to sanctions and export restrictions on technology and software. First, the particular sanctions regulations of the EU and the US with regard to the technology and software will be examined with an emphasis on the design of the legal norms and general approach. For sake of brevity, the analysis will be limited to some recent or most prominent examples of sanctions norms.

Second, the relevant issues relating to the jurisdiction of sanctions legislation will be addressed, primarily the disputable question of extraterritoriality and the importance of the origin of objects for the definition of jurisdiction.

3.1 Design of restrictions relating to technologies and software

The EU has a consistent policy on the wording in the sanctions legislation and, as an example, the main and recently amended acts will be examined, namely the Sanctions Regulation[22] together with Council Decision 2014/512/CFSP[23] and the Dual-Use Regulation[24]. These acts invariably use the term "goods and technology" thus merging in one category a variety of subject matters, from raw materials and equipment to software and know-how.

Based on an analysis of the provisions of the Annexes to the Sanctions Regulations one can conclude that EU sanctions on technology (financial sanctions of any kind are out of the scope of this paper) are for the most part related to tangible objects, primarily machinery and equipment (for example, drilling platforms, aircrafts, vessels, marine systems, and equipment). Technology is rarely mentioned as a prohibited item as such, only occasionally in relation to specific sanctioned industries (for example, refinery fuel gas treatment and sulfur recovery technology).

[22] Council Regulation No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2014] OJ L 229/1 (Sanctions Regulation).
[23] Council Decision No 2014/512/CFSP of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2014] OJ L 229/13.
[24] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [2021] OJ L 206/1 (Dual-Use Regulation).

The same applies to software. Restrictions are mostly related not to software or technology as such, but to their application (with regard to software the term "specially designed" is used) for the "development", "production", or "use" of sanctioned goods.[25]

This limitation may even seem excessive regarding complex equipment. The technology and the software controlling it usually form a whole and are supplied as a package, and in the absence of the controlling software, the equipment cannot function. However, in other cases, the underlying technology or software may be even more important than the physical medium, and lack of access to the software or technology makes it impossible, for example, to reverse engineer or continue to use existing equipment in a sanctioned State.

It should be noted that in the EU, in sanctions against Russia, as mentioned above, the software is rarely listed as a separate prohibited export item, and that is probably why there are no criteria regarding the technical details of permitted or prohibited software. Accordingly, the specifics of FOSS are not taken directly into account by the Sanctions Regulations, which is understandable given the general emphasis on tangible objects.

Still, these issues are not ignored completely. For example, the Dual-Use Regulation provides the carve-out from export control regimes on technology transfer with regard to information in the "public domain" or to "basic scientific research" (Annex I). However, it should be noted that the "Whereas" section of the Dual-Use Regulation (clause 13) refers primarily to the interests of academia. Though for sure FOSS may be used, *inter alia*, for the purposes of scientific research, it is not the primary aim.

It is also important to note, that despite the Dual-Use Regulation carve-out on the "public domain", there are no similar provisions in the Sanctions Regulation, although both Regulations address the export of technology and software. Therefore, it is not evident if the exports of goods and technologies controlled under the Sanctions Regulation may apply this provision by analogy. The issue of the "public domain" carve-out and its applicability to FOSS will be addressed in detail below in section 4.1.

[25] It should be noted that regulatory options even under the Sanctions Regulation are more complex and various. Three cases, in particular, can be distinguished: (1) software and technology are restricted to the extent they are used for "development", "production", or "use" of sanctioned goods (a most common regulatory approach with regard to the list of goods in Annex VII to the Sanctions Regulation), (2) software and technology are restricted from export as such, (3) expansion of the Dual-Use Regulation by means of restricting the export of software and technology relating to the regulated dual-use goods. Moreover, the Sanctions Regulation contains different Annexes where different approaches are applied to establishing the list of restricted goods and technologies. In some cases, the list is based on the Common Customs Tariff and Combined Nomenclature (CN), which makes it more feasible for the users. In other cases, CN code is not indicated. In relation to one of the most voluminous and complex Annexes, Annex VII, consisting of the "goods and technology which might contribute to Russia's military and technological enhancement, or the development of the defence and security sector", the European Commission made the Correlation table with CN codes. However, neither software nor technologies are included in this table. As the Commission explains with regard to the technologies, "*the export of intangible items is not declared at Customs*", and for software either the CN code of the relevant equipment there is embedded is used, or "*most of the times software is not sent to the recipient through Customs but through the cloud, or by means any computing server*". See Annex – Indicative temporary correlation table for items listed in Annex VII of the Sanctions Regulation to "Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014". While this explanation sounds logical, it does not make it easier for users to correctly determine whether or not a particular technology or software is allowed to be exported.

US sanctions laws can rightly be considered the most detailed and developed. Sanctions have long been a regular part of US foreign policy. Sanctions legislation has long been in the making[26], is extensive and still so structured that some other countries that impose sanctions through "one-off" emergency acts can use it as a model.

US sanctions are truly all encompassing; the same events or persons may be targeted by up to four different types of sanctions: listing of the individuals and companies on the Specially Designated Nationals (SDN) list[27] (which makes them "untouchable" as any transaction with these persons is prohibited), Sectoral Sanctions related to particular sectors of the economy (for example, in the case of sanctions against Russia one of the targeted sectors is oil and gas), Geographic Sanctions related to transactions with particular States and/or regions (there are different sanctions relating to Russia and to Crimea) and finally Secondary Sanctions (which may be imposed on non-US persons doing business with sanctioned individuals).[28]

Despite such a variety, US sanctions are based on two main sets of lists that are to be used by any US (or even non-US) national for evaluation of the possibility of doing any business with representatives of the sanctioned State: lists of sanctioned entities and Export Administration Regulations (EAR).[29] In practice, most US sanctions are linked to an extensive and very detailed EAR, so, in order to determine if a product may be exported to a targeted State, it is necessary to check first if the targeted product falls under export control regulations, and then, – whether there are any restrictions relating to the targeted State or a specific buyer therein.

The main body which regulates and enforces US economic sanctions restrictions against designated parties is the Office of Foreign Assets Control (OFAC) in the United States Treasury Department. Given the close relationship between sanctions and export control, another important official body is the Department of Commerce's Bureau of Industry and Security (BIS), which regulates and enforces U.S. export controls under the EAR and, in particular, issues export licenses.

Issues relating to technologies and software are regulated in great detail by the EAR, and sanctions legislation simply contains references to EAR provisions. In comparison to the EU approach, the US regulates software issues very extensively, with a lot of technical detail.

Characteristically, the EAR clearly distinguishes between software and technology and in some cases treats them differently. Again, this distinction depends on the technical

[26] Gary Clyde Hufbauer and others, *Economic sanctions reconsidered* (3rd edn, Peter G Peterson Institute for International Economics 2007) 11; Michael P Malloy, 'Contracts and Economic Sanctions' (2022) 53(3) University of the Pacific Law Review 617.

[27] Specially Designated Nationals And Blocked Persons List administered by OFAC <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists> accessed 18 February 23.

[28] Secondary sanctions are a rather controversial matter and will be discussed below with regards to extraterritoriality.

[29] US Department of Commerce, Bureau of Industry and Security, Export Administration Regulations <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear> accessed 18 February 23.

details. This is also understandable given that the US is the undisputed world market leader in software and corresponds to the standard approach according to which the sanctioning State is likely to enjoy a dominant market position as a supplier.[30]

The EAR does not indicate the term "FOSS" or other similar terms directly, however, in other aspects provides a far more detailed regulation than EU sanctions law. According to the general rule, if technology or software is "publicly available", it is outside the scope of the EAR.[31] The term "publicly available" compared to the term "public domain" used in the EU legislation is more neutral as there is no such term in international legal doctrine and therefore it cannot be misleading. It may be contended that the term "publicly available" is more apt for the purpose, especially since the EAR explains in detail its meaning. Furthermore, the EAR uses the term "published", which means that technology or software "has been made available to the public without restrictions upon its further dissemination". Particular ways of publishing are also indicated. For software and FOSS, in particular, the most suitable criterion is "public dissemination in any form including posting on the Internet in sites available to the public".

However, the US would not be the US if it would simply exclude FOSS from export controls and thus from the scope of sanctions. We will look more closely at the specifics of applying sanctions to FOSS in section 4.1.

3.2 Approaches to the jurisdiction of sanctions: extension of sovereignty

The question of which individuals and which goods (services, technologies) are subject to sanctions is one of the most pressing. Globalisation has led to goods and components (together with embedded technology and software) being produced and resold between multiple States, involving transactions not necessarily implicating nationals or companies from those States. Globalisation is a major challenge for a State trying to impose sanctions, especially in the technical field.

The EU and the US approaches to jurisdiction over sanctions are fundamentally different, and the tensions between them essentially reflect the tension between the classic approach to jurisdiction, historically accepted in international law, and the innovative approach focusing on expanding the jurisdiction.

The EU approach to sanctions jurisdiction is a fairly standard combination of national and territorial principles: on the one hand, sanctions apply within the jurisdiction (on EU territory) and, on the other hand, to all EU citizens or companies incorporated under EU law. In essence, this approach is no different from the way any national legislation normally operates. The EU applies it deliberately, and specifically stresses that "*the EU*

[30] Hufbauer (n 26) 91. It should be noted also that the US President has more powers with regard to export than to import, which is yet another reason for very extensive export restrictions.
[31] §732.2, §734.7 EAR.

refrains from adopting sanctions having extra-territorial application in breach of international law".[32]

The US approach is fundamentally different: US sanctions are extraterritorial, as they impose compliance obligations not only on US nationals but on any person in any other State who may engage in transactions with the sanctioned States or individuals. *De facto*, this provision is backed by the statutory possibility to impose secondary sanctions on any non-complying person.

This approach gains a particular significance with regard to cyberspace (including operations with FOSS) because if anyone in the world has any degree of control over it, it is likely to be the US. It may be argued that the US actually exploits the absence of adequate international regulation of jurisdiction over the Internet in order to implement its national law and thereby extend its rule.[33]

The justification for the extraterritoriality of US sanctions is interesting *per se*. Extraterritoriality is usually justified by an extension of the nationality principle. However, this only applies, for example, to the application of the law to companies established by nationals abroad, which is not the case.[34] Neither can the effects doctrine (based on the significant domestic effect of the actions performed abroad) be applied here.[35]

It is noted in the academic literature that extraterritoriality generally calls into question the legitimacy of the legislation.[36] And for US economic sanctions, there is in principle no justification recognised in international law. Unsurprisingly, most countries consider this illegal and even try to oppose it. As early as the 1980s, US allies wondered at whom the US sanctions were aimed in the Soviet-European gas pipeline case, and the infamous Helms-Burton Act of 1996 against Cuba provoked outrage even among US allies.[37]

The extraterritorial nature of US sanctions has been criticised primarily for affecting the sovereignty of the other States[38] and even challenging it[39] by means of overstepping jurisdictional boundaries[40] and even establishing a hierarchy among States (which

[32] European Union Sanctions <www.eeas.europa.eu/eeas/european-union-sanctions_en> accessed 14 February 2023.
[33] Henning Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (2021) 32 Duke Journal of Comparative & International Law 61.
[34] Iryna Bogdanova, *Unilateral Sanctions in International Law and the Enforcement of Human Rights* (Brill/Nijhoff 2022) 91.
[35] Mark Daniel Jaeger, 'Circumventing Sovereignty: Extraterritorial Sanctions Leveraging the Technologies of the Financial System' (2021) 27(1) Swiss Political Science Review 180.
[36] Sergey Glandin, 'Экстерриториальность американских санкций в действии' [US sanctions extraterritoriality in action] (2018) 2 Международное правосудие [International justice] 105.
[37] Hufbauer (n 26) 9.
[38] Steven Blockmans and others, 'Extraterritorial sanctions on trade and investments and European responses' (2020) <www.ceps.eu/ceps-publications/extraterritorial-sanctions-on-trade-and-investments-and-european-responses> accessed 21 February 2023.
[39] Jaeger (n 35).
[40] Bogdanova (n 34) 90.

contradicts the principles of sovereign equality embedded in the Charter of the United Nations).[41]

The EU not only denies the legality of extraterritorial sanctions, but actively opposes it. The Blocking Statute[42] was adopted to protect EU nationals against the effect of extraterritorial sanctions. Switzerland has gone even further by criminalising to some extent compliance with foreign sanctions on Swiss territory.[43]

Finally, the extraterritorial nature of US sanctions was discussed and disapproved of several times at the United Nations.[44] But all this was to no avail since US sanctions are still in place and are complied with, even by EU players protected by the Blocking Statute. This may be logically explained by the high interest of international players in the US market as well as by a high level of interdependence in a particular market, specifically the financial one. The biggest players comply with US sanctions because, for most part, they have US-based businesses, and the sums of fines imposed by the authorities are significant; meanwhile, smaller players have to comply with sanctions because of the bigger ones since it is far more practicable to arrange similar compliance procedures all along the same chain.[45]

It is also rightly observed that over-compliance is a general practice.[46] Though in some cases it is impossible to make the market players comply,[47] they still can be nudged to comply based on the actual balance of the world powers.[48]

Despite the principle of sovereign equality of States proclaimed by the UN Charter, the real world of sanctions is an asymmetric one: the hegemonic States are free to use extraterritorial sanctions without fear of reprisal.[49] J. Benton Heath has stated, "*the world according to targeted sanctions doesn't look much like a geographic map at all, but a network*"[50] and this seems correct.

Furthermore, it would be even more correct if we take into consideration not just the formal extraterritoriality expressed in the US secondary sanctions, but the approach to setting the list of goods and services subject to export control. The EAR stipulates two particularly specific types of provisions on it, namely the "de minimis" rule and "direct

[41] UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Idriss Jazairy (2015) A/HRC/42/46.
[42] Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom [1996] OJ L 309/1 (Blocking Statute).
[43] Jaeger (n 35).
[44] UN General Assembly Resolution (2019) A/RES/74/7.
[45] Jaeger (n 35).
[46] Edoardo Saravalle, 'Bargaining Chip? On the speed and scope of the Russia sanctions, and the prospects for off-ramps' (2022) Phenomenal World <https://www.phenomenalworld.org/analysis/bargaining-chip> accessed 16.02.2023.
[47] Hufbauer (n 26) 175.
[48] Chiara Franco, 'Coercive Diplomacy, Sanctions and International Law' (2015) <hwww.iai.it/en/pubblicazioni/coercive-diplomacy-sanctions-and-international-law> accessed 17 February 2023.
[49] I N Timofeev, 'Экономические санкции как политическое понятие' [Economic sanctions as a concept of power politics] (2018) 2(59) Вестник МГИМО-Университета [MGIMO Review of International Relations] 26.
[50] J Benton Heath, 'The Possible Worlds of Economic Sanctions' (2022) Temple University Legal Studies Research Paper 05/2023 <https://ssrn.com/abstract=4254455> accessed 13 February 2023.

product" rule. According to the "de minimis" rule, not just items produced in the US are subject to export control, but also items produced abroad containing some percentage of US components (including US technology and software) (art. 734.4 EAR). Similarly, the "direct product" rule provides that foreign-produced items located outside the US are subject to the EAR when they are a "direct product" of specified "technology" or "software" subject to the EAR (art. 734.9 EAR). A recent example of the application of these restrictions is the US-China trade war: as the result of sanctions based on "direct product" rule, Huawei was completely prevented from purchasing the chips containing US technology.[51]

Such an approach dramatically enlarges the scope of export control (and thus sanctions) regulation of the US without formally affecting jurisdiction.[52] It may be contended that these norms are even more important than the disputes over secondary sanctions, as they help the US to expand its influence around the world virtually invisibly, and there seems to be no contradiction with international law (or at least the contradiction is not that evident as in the case of secondary sanctions).

4 Application of sanctions to FOSS: colliding sovereignty trends

4.1 Practical challenges of sanctions application to FOSS

As it was recognised by the UN Group of Governmental Experts, international law applies to digital space.[53] But this is not the case for specific websites, which may usually be easily linked to the jurisdiction of a particular country, based on the owner's origin. If the owner is not indicated on the website it can be defined by using the WHOIS service, based on the domain name registration State and/or the State of the hosting provider.

It should be noted that the majority of the most popular FOSS websites fall under the jurisdiction of the US. The Linux Foundation is registered in California[54] and thus would comply with US sanctions. GitHub, probably the most popular website for software developers, though regarded by many as "sanctions-neutral" in fact directly stipulates in its Terms that "*access to or use of the Website or the Service are governed by the federal laws of the United States of America and the laws of the State of California, without regard to conflict of law provisions. You and GitHub agree to submit to the exclusive*

[51] Bogdanova (n 34) 102.
[52] It may be interesting to compare this new public law approach to the long-established private law one with regard to the rights to the technology embedded in a tangible object. It is worth reminding that an international doctrine of exhaustion of IP rights started from a famous US case Adams v. Burke, 84 U.S. 453 (1873). Nowadays we can see how the US government tries to prolong its rights to control the objects far beyond based on the same embedment of technology.
[53] Report of the UN Group of Governmental Experts 2012/2013 adopted by the UN General Assembly Resolution A/RES/68/243.
[54] The Linux Foundation Terms <www.linuxfoundation.org/legal/terms> accessed 18 February 2023.

jurisdiction and venue of the courts located in the City and County of San Francisco, California".[55]

Furthermore, the owners of the relevant websites may implement policies restricting the use of materials, including FOSS, even if they are not obliged to comply with the sanctions of the relevant State. Generally, this will be stated in the Terms of Service for the website.

In early 2022, GitHub blocked a number of developer accounts from Russia and even deleted their commits, causing outrage in the community.[56] Thus, even an international and usually politically neutral FOSS community or a specific website may support the sanctions either due to a direct legal obligation or due to the personal political position of the owners. However, in general, such actions go against the culture of the FOSS community, and it must be agreed that the resilience of software ecosystems to threats against their culture is important to become sustainable.[57] Taking into account the high level of connection between contributors from different States to create the final integral product, no software community may allow discrimination beyond what is directly prescribed by law. This approach is also envisaged in the principles of the Open-source initiative.[58]

As indicated above, EU sanctions provide a carve-out for the information in the "public domain". However, it is not evident how the "public domain" should be matched with various types of FOSS licences. Generally, intellectual property law distinguishes "public domain" regulation from any type of licensing. The public domain usually covers IP items with the expired term of protection (a common example here would be classical literature) or those specifically transferred into the public domain by the author. At the end of the day a licence that is enforceable before courts is something that directly contradicts the idea of the "public domain".

However, there are Recommendations from the EU Commission[59] that provide a broader interpretation of "public domain" status for the purposes of the Dual-Use Regulation: "*Technology or software which has been made available without restrictions upon its further dissemination*".

Clause 2.3.5 of said Recommendations envisages two main criteria for a de-control application under "public domain" rule. Firstly, software should have already been made available to the public. Basically, it means that de-control is easily applicable to the open-

[55] GitHub Terms of Service <https://docs.github.com/en/site-policy/github-terms/github-terms-of-service#r-miscellaneous> accessed 18 February 2023.
[56] It should be noted that later GitHub changed its policy, and now officially states that it is available to developers in all countries, and they are continuing to ensure free open-source services are available to all, including developers in Russia, see <https://github.blog/2022-03-02-our-response-to-the-war-in-ukraine>.
[57] Kula and Treude (n 20).
[58] The Open-Source Definition <opensource.org/osd> accessed 20 February 2023.
[59] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items [2021] OJ L 338/1.

source software released earlier than the Dual-Use Regulation. But what about the new open-source software, which is continually produced by the community? The situation is not that clear in this regard. The Commission clarifies that henceforth, the act of releasing without authorisation can be a violation of export controls. Such an approach, though formally correct, creates a set of problems for a legal practitioner. If a developer released version 1.0 before the Dual-Use Regulation came into force, it does not require export control. But what about versions 1.1 or 2.0 released after the Regulation? Are they regarded as the "same software" or "new software" for export control purposes?[60] However, this criterion is not as controversial as the second one.

According to the clarifications of the Commission, the second criterion for the "public domain" rule is that the software was "*made available without restrictions upon its further dissemination (copyright restrictions do not remove 'technology' or 'software' from being 'in the public domain')*". Though this requirement is absolutely feasible for the "classic" public domain, it poses some significant difficulties in relation to open-source software. The wording of the Commission is identical to the wording of the EAR on the same issue. However, unlike the EAR, which provides detailed options for publishing "without restriction upon further dissemination" and even gives examples, neither the EU legislation, nor clarifications of the Commission contain similar degree of detail.

The term "public domain" considered in conjunction with FOSS specifics may lead to ambiguity because strictly speaking FOSS is not a public domain and copyleft licences actually provide significant restrictions on further dissemination of modified software. Moreover, the carve-out is provided only in one Regulation (Dual-Use), and it is not evident if it can be invoked in connection with the application of the Sanctions Regulation.

Therefore, EU sanctions legislation (subject to the limitations on the scope of the analysis indicated above) lifts export restrictions from technology and software upon certain conditions. However, it cannot be unequivocally concluded that this exception applies to the whole of FOSS in its diversity. The lack of detail in the regulation (which necessitated the issuance of clarifications by the Commission) of FOSS complicates the practical implementation. No cases of liability for breach of EU sanctions in relation to FOSS have been identified, but it cannot be concluded that developers and users of FOSS should not take the sanctions into account at all.

The US sanctions relating to FOSS are particularly dangerous for users because they impose several additional restrictions which must be complied with and failure to comply with them will result in liability.

While no prosecutions have been found specifically in relation to the illegal export of FOSS, a similar practice on proprietary software exists. In 2021, a German software

[60] This is a general question posed with regard to all situations where distinguishing between different software released as between different (or same) commercial objects is important for the lawyer. In absence of a specific regulation of the legislation, the answer usually depends upon the lawyer's discretion and the position of the developer on the amount and importance of changes made within the new release.

company was held liable for US sanctions violations, as it sold software licenses in Turkey, the United Arab Emirates, Germany, and Malaysia, but further, these software licences were resold via cloud service to Iran (a State heavily sanctioned by the US). The total fines and mediation expenses amounted to more than 30 million US dollars.[61]

Such high penalties for sanctions violations, quite typical for the US, require all users (exporters and importers alike) to pay the utmost attention not only to the basic requirements of the law but also to exceptions which are stipulated in the EAR. Despite the general indication in the EAR that publicly available software is not subject to export restrictions, it takes at least five steps to be conclusively convinced:

Step 1: Check if FOSS meets the criteria of being "published" according to §734.7 of the EAR.

Step 2: Check if software or technology is intended for the production of a firearm, or firearm frame or receiver, and controlled under a particular ECCN code. If yes, the EAR will still be applicable even to FOSS. Of course, firearm production is a quite rare application of FOSS, but this exclusion should still be noted for the sake of completeness.

Step 3: Check if FOSS includes any type of encryption. If not, FOSS will be out of scope of the EAR and of sanctions. However, "encryption software" is defined by the EAR quite broadly (for example, it covers the software that merely activates encryption features in another software or hardware),[62] therefore special attention is required at this step. In practice, such a check may be problematic if it is a potential user and not the developer who tries to comply with sanctions. In the absence of any comments from the developer, it would require the user to perform an analysis of the code and therefore spend additional time and resources on it.

Step 4: Check if the encryption is standard or not. This step may be a challenge even for a developer since there is no unified international notion of "standard cryptography". However, the EAR gives some ideas on possible approaches: according to the official definition, "standard" cryptography algorithms are supposed to be approved by a duly recognised international standards body or otherwise published.[63] It should be noted, that according to the Linux Foundation, non-standard cryptography is a rare thing in an open-source project.[64] But still, the risk may be too high to exclude the possibility without checking.

Step 5: In case of non-standard encryption, a preliminary notification is to be filed by the developer of FOSS to both BIS and the National Security Agency (§ 742.15 EAR). In absence of the notification publishing FOSS may also constitute a violation of sanctions since the developer cannot control if its software is downloaded from abroad or not.

[61] Thorsten J Gorny, 'Why OFAC Sanctions Compliance Is Important for Software Companies' (Sanctions.io, 14 December 2021) <www.sanctions.io/blog/why-ofac-sanctions-compliance-is-important-for-software-companies> accessed 18 February 2023.
[62] Winslow (n 2).
[63] §772.1 EAR.
[64] Winslow (n 2).

Moreover, a potential user should also care to check if such notification was sent and if evidence is provided by the developer to exclude its own risks. Generally, if there are no comments from the developer a potential FOSS user from a sanctioned country will face the challenge either of accepting the risk or of refusing this FOSS.

In general, the set of additional checks that a developer and a user need to pass in order to definitively verify that the FOSS is not subject to export restrictions is quite onerous. Thus, the initial impression that FOSS is not subject to US sanctions is not correct. Moreover, the complexity and detail of the regulation, both legally and technically, require significant investment in compliance alone. Of course, it does not completely block the possibility of use of US-origin FOSS even for States subject to US sanctions and embargoes, but still, additional requirements and regulations are an additional burden for both developers and users, thereby reducing the efficiency of FOSS.

Furthermore, the very fact that the export laws of the world's largest economy are so technically detailed in their regulation of FOSS shows, first, the level of State involvement in these issues and, second, the political will to regulate them (while the EU lacks it, given that it has settled on a general exclusion of the public domain from sanctions restrictions).

This political will is worrying because it does not exclude the possibility that new requirements could be imposed by the EAR to make it illegal to distribute a higher percentage of FOSS around the world. This would have a negative impact on the viability of FOSS as a framework, given its international nature.

4.2 Sanctions and FOSS: erosion or broadening of sovereignty?

In today's world new trends emerge, collide with each other, and bring about the next trends, often opposing ones. When considering trends in sanctions and trends in the technologies (in the broadest sense, including the FOSS framework as well) it becomes clear that they are opposing each other. Both these spheres (sanctions influence and technological neutrality) are expanding, and although at first glance they exist in different worlds, at some point they will collide.

The issues of jurisdiction and sovereignty are the main ones in relation to emerging technologies. Traditionally, international law acknowledges national and territorial principles of jurisdiction. Additionally, there are internationally acknowledged precedents of legal extraterritoriality, for example, the effect doctrine (when action abroad has a significant effect in a particular State) or universal jurisdiction (first of all, with regard to international crimes).

However, the erosion of sovereignty due to the development of new technologies, above all the Internet, can hardly be denied. Modern technologies are creating unique types of objects that are essentially extraterritorial and often cannot be properly regulated by any legislation. These are not only FOSS, but also cryptocurrencies, assets in the Metaverse, NFTs, etc. It is sometimes technically impossible to control such types of

objects for the State imposing the sanction, thus compliance with sanctions becomes more of a good faith exercise for the private entities who are in charge. Still, in some cases, control is not achievable due to the very nature of the objects, for example, the inherent level of anonymity as both a technical basis and the main feature.

Of course, the answer to expanding sanctions is to find ways to avoid the associated restrictions, for example by using cryptocurrencies[65] or other new technologies, FOSS included. As Barry Eichengreen correctly observed, military power is concentrated, whereas economic power is disbursed,[66] that is particularly true with regard to cyberspace and the interaction of the online community. Governments imposing sanctions can try to force companies to comply with them, but doing so with a distributed community comprised of individuals is more difficult. The decision to support or not support sanctions is not only based on economic considerations but also on shared community values.

On the other side, the States commence implementing sanctions in spheres which were historically neutral, such as international finance. Whereas in previous centuries countries sometimes continued to pay their debts to their enemies in the face of an ongoing war, the opposite is more likely to happen now. The sanctions penetrate the international finance world and weaponise it,[67] so perhaps one can agree with the statement that "global trade and finance now serve as key battlegrounds of modern warfare".[68] It cannot be denied, however, that financial globalisation has to some extent deprived States of influence in this very traditional sphere and has also contributed to the erosion of sovereignty, so by intruding with sanctions regulation in this sphere the States are regaining this partially lost sovereignty.[69]

The same is relevant for FOSS. From its inception in the 1980s, States did not deal with FOSS specifically and did not attempt to regulate it, given that FOSS does not deprive States of any pre-existing spheres of control. However, with the expansion of sanctions and their extension to fundamentally new spheres of relations, the FOSS has also come under the regulatory scrutiny of the most advanced State in sanctions area, i.e. the US.

Nowadays, States tend to start regulating (or at least trying to regulate) the spheres which never before were subject to State control, in particular, areas that previously seemed to be exclusively international. It seems that we have moved away from classic territorial jurisdictions into cyberspace, the world of data transmitted by electrical signals, which cannot be stopped at customs. However, State jurisdictions follow close behind the technologies, catching up and sometimes overtaking them. Moreover, it can

[65] In particular, the digital yuan launched by China will free China's international payments from US control (given that most payments are still made in dollars) and reduce geopolitical and financial risks, see Arner (n 15).
[66] Barry Eichengreen, 'What Money Can't Buy. The Limits of Economic Power' (2022) *Foreign Affairs* <https://www.foreignaffairs.com/articles/united-states/2022-06-21/what-money-cant-buy-economic-power> accessed 15 February 2023.
[67] Heath (n 50).
[68] Arner (n 15).
[69] Pierre-Hugues Verdier, *Global Banks on Trial. U.S. Prosecutions and the Remaking of International Finance* (OUP 2020) 107.

be argued that such an expansion of jurisdiction was invoked by the recently arisen technical ability to freely transfer valuable information (whether in the form of personal data or technology) across borders.

Based on the approach to sovereignty in cyberspace, States are usually divided into two groups: Western democracies, headed by the US and representing the ideas of the Internet without borders and free flow of information, and a bloc of mostly Eastern countries like Russia, China, and Iran, which advocate for a sovereign Internet and the right of the State to regulate access to information. But this discourse seems to be outdated and too formal. It is more an official position presented at the UN level rather than the real state of affairs. Based on the practical approach to controlling the Internet the classification suggested by Henning Lahmann seems more relevant, between "cyber-imperialism" (including the same set of Western countries, first of all, the US) and "cyber Westphalia" (the same "Eastern bloc", primarily China and Russia).[70] In this interpretation, "cyber-imperialism" loses its democratic gloss and becomes a more accurate reflection of the real US cyberspace policy, based on the high degree of control over the critical elements of the ecosystem (starting with root servers) and extraterritoriality of sanctions, *inter alia*, in the IT sphere.

States implement new ways to control new technologies not for the sheer purpose of control but rather in order to (re)assert their jurisdiction. Initially neutral digital space is starting to be regarded as "no man's land", so the first State (or States) to gain the effective (not obligatory legally justified) control over it may as well be deemed to assert their "digital sovereignty".[71]

The obvious bidder is, of course, the US, therefore, it is not surprising that not only developing countries but also the EU have started talking about their own "technological" or "digital sovereignty" relying among other things on the classic legal approach to sovereignty, which is closer to the "Westphalian" paradigm than to the "imperialistic" one.[72] Still, it cannot be ruled out that notwithstanding the formal criticism of the US extraterritorial approach, other States will not try to follow it. New legal methods are employed for the reassertion of the State sovereignty over the new technologies.

Both EU and US legislation exempt FOSS from sanctions. However, US law introduces an exception to the exception, setting out the conditions under which FOSS would still be subject to export control and sanctions. It is a complicated legal model, based largely on technical details, so its "imperialistic" character is not as evident as in the case of more straightforward secondary sanctions.

A new model of this sovereignty extension exploits the notion of components, originating or otherwise related to the sanctioning State. This is a new jurisdiction and even new form of extraterritoriality. Completely new criteria for definition of the jurisdiction are starting to appear in legislation, based on embedding into the goods

[70] Lahmann (n 33).
[71] ibid.
[72] ibid.

(understood as broadly as possible), services, technology, and even simply information of the components originating from a particular State. Thus, national legislation (including export restrictions) follows an object (both tangible and intangible) across borders and continues to be effective in the territory of other States.

Whereas in the past jurisdiction was linked only to persons (natural or legal) and territory, now it becomes linked to different types of objects. Such an approach may cause significant challenges, first of all, for international trade, and secondly, for the free flow of information.

This is mainly, but not exclusively, US legislation. For a change, the controversial EU General Data Protection Regulation (GDPR)[73] may be recalled. Because of its application to the personal data of European individuals regardless of the State in which the data is processed it well deserved to be called an expression of European "judicial imperialism".[74]

The pretext of protecting citizens' rights (the case of the GDPR) is of course more benign than purely economic or even purely political considerations, but it does not negate the similarities in substance.[75] In practice, especially when it comes to components in the final product, it is very difficult to properly assess the necessity of applying such norms. Moreover, if such legislation is adopted by several States with opposing export regulations, the product containing components from both States will likely become untradeable. Big Data may become a completely useless and even toxic asset in cases when some specifically protected information (like the personal data of EU nationals) is included in the dataset.[76]

This contributes essentially to an anti-globalist trend in legislation, which may have a profound negative impact on international trade and data flow. Moreover, such an approach to the jurisdiction reveals an effort of the states to reaffirm sovereignty and to reply to the threats of sovereignty erosion posed by the free flow of information through the Internet and of goods and services across the borders.

In this regard, the third State's sovereignty becomes an issue. It is generally accepted that territorial sovereignty includes, *inter alia*, prohibition for a State to exercise its power on the territory of another State. But the type of jurisdiction which follows the object does not recognise the State borders. It is questionable whether there are effective mechanisms to coerce or at least to regulate this jurisdiction expansion, and whether they are needed. Given that the strongest States in the world are involved, the balance of

[73] Regulation of the European Parliament and of the Council No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).
[74] Lahmann (n 33).
[75] We can only hope that China would not decide to try the same approach, for example, for all manufactured electronics.
[76] As Steven Blockmans carefully observes in the report 'U.S. Clarifying Lawful Overseas Use of Data Act', a.k.a. CLOUD Act which gives American law enforcement authorities the power to request data stored by most major cloud providers may raise potential conflicts with GDPR (n 39). This will be exactly the case of the collision of two de facto extraterritorial norms.

power is certainly decisive.[77] On the other hand, technologies continue to evolve and are likely to proceed within the deregulation trend.

As for the position of other States, we will probably see two tendencies: the most powerful States where multinational corporations are eager to carry out business will impose their extraterritorial legislation using these types of norms. While weaker States are more likely to impose a strict control over national actors, goods, and datasets in order to prevent the applicability of foreign legislation.

It may become a challenge for multinational corporations to comply with the laws of all the States where they operate. Whereas nowadays it is often necessary to set up different processes and controls for different countries, which in itself is costly, in the future, it may happen that the same software or dataset will be subject to possibly contradicting laws of several States simultaneously. As a simple solution, a company may choose to comply with the legislation of the most important State of business with the highest penalties.

However, the best solution would be an international regulation relating to the legality and compatibility of such extraterritorial norms.

5 Conclusion

The analysis shows that even a politically and technologically neutral phenomenon such as FOSS is not entirely free from State regulation, including sanctions regulations. At the same time, FOSS in its inherent characteristics is quite in line with the general trend towards de-regulation, overcoming State borders and sovereignty, commonly associated with other phenomena in cyberspace. This trend relating to the technical characteristics of new objects will certainly continue.

However, it is too early to write off the State as such, and the analysis of the sanctions regulations already demonstrates this. It would be wrong to expect the most powerful States to agree to lose control over the important areas in economics only because transactions related to these spheres have been transferred to cyberspace and are now performed via emerging technologies. On the contrary, as the analysis of US sanctions legislation suggests, the State tries to follow such objects into cyberspace as well, introducing new approaches to legal regulations. Therefore, the expansion of the jurisdiction, as demonstrated by examples from US and EU practices, can be called an opposing trend.

It can be assumed that these practices will evolve and the quality of legislative techniques in terms of new technologies will increase. Technical innovations, which

[77] Akbar Adibi and Homayoun Habibi, 'The Challenge of the "Economic Independence" and the "Sovereignty of States": A Review of the Problem of Legitimacy of Economic Sanctions in the Reality of the International Legal Order' (2017) 5(3) Russian Law Journal 113.

initially remained in a grey area for the legislator, will be regulated as their economic importance grows.

In general, it resembles a game of chess: technological advances give birth to new phenomena, processes, and opportunities beyond the scope of existing legislation. States (to a different degree, of course) respond by seeking ways to regulate these new phenomena in order to safeguard national interests and reassert their sovereignty. Moreover, approaches applied to extend the jurisdiction of States constitute new legal practices. First of all, it is relevant for cases where State jurisdiction (and in particular sanctions prohibitions and restrictions) follow the object of regulation even if it is not located in the territory of that State (through the application of the "national origin" criterion).

Apart from the political implications, these practices are likely to be questionable from the perspective of international law based on the classic UN Charter approaches, *inter alia*, prohibition to exercise the power on the territory of another State. The situation becomes even more complex when it comes to intangible objects transmitted via the Internet, such as datasets or software. If such State practices become more popular and widespread, it will be somewhat of a challenge to the generally accepted model of State jurisdiction and an interesting task for legal practitioners.

*Diego Saluzzo**

"BIG TECH" RESPONSIBLE BUSINESS CONDUCT

Transparency and due diligence obligations for online platforms and safer space for online users' fundamental rights, now and in the Metaverse

Abstract

Platform economy has substantially changed traditional business organization, market structure and contractual power relations. Digital platforms in fact impose their terms to all the users: no room for negotiation and reduced ability of the traders to influence the rules of the game. The positive fact is that digital platforms have strong interest in reducing risks and guaranteeing safe transactions. For such a reason the U.S. legal system - used to facilitate running business, with no overruling approach - adopted a "*laissez faire*" approach. European approach, on the contrary, is aimed at regulating digital markets and Artificial Intelligence ("AI"), on which relevant transactions are based. Insofar contracts are concluded in a condition of unequal contractual power to the advantage of platforms, disparities should be countered, at least to safeguard users' fundamental rights. In a marketplace governed by obscure algorithms public control is extremely difficult and, for such a reason, self-regulation becomes crucial. That applies not only to current scenario, but also to the incoming Metaverse dimensions under establishment, which offer room enough for fixing appropriate rules of engagement between digital platforms on one side and private and professional users on the other side, for the benefit of end users worldwide. Responsible Business Conduct ("RBC") is so expected to evolve also at Metaverse level, with an AI systems' structure that must comply with rule of law and respect human rights, democratic values and diversity. All that originated from OECD evidence-based international standards. Platforms are so expected to be more and more transparent and accountable and applicable regulations are increasingly focusing on good faith efforts to protect centrality of fundamental human rights *vis-à-vis* Big Techs. The question is if self-regulation and ethical guidelines and standards could really represent safeguard enough against bad and unproper use of AI also in the on-going Metaverse development, where fundamental human rights are and must remain central, by avoiding and sanctioning any sort of manipulation or harm. That represents a new test field for the legal community everywhere in the world, namely in terms of law enforcement, where the Metaverse has potential to provide many benefits, namely including telecommuting, matchmaking, and preservation of data, but also possibility to add new and unregulated risks.

* Grande Stevens Law Firm, Turin, Italy. This manuscript is the result of a very productive meeting held in October 2022, which brought together lawyers, academics and technical partners. The consultation was held at a seminar presented by the Unione Internationale des Avocats (UIA) with the support of the Brussels Bar, in collaboration with hub.brussels, the Brussels Agency for Business Support titled "Law Versus Digital Technologies: A Necessary Alliance? Legal, Economic and Environmental Opportunities and Challenges". Some of the presented results have already been published by my colleague Jan Mulligan, at that time chair of the UIA's Health Law Commission, on her website as reported in the references, and some other data presented at that time, with reference to drug device technologies, by my colleague Eliana Silva de Moraes, current chair of the UIA's Health Law Commission. I would like to thank also to my colleague Carlos Ramirez, who completed our successful panel in Brussels.

JEL CLASSIFICATION: K20, K24

SUMMARY

1 Platform economies: the new rules of the game

Platform economy has substantially changed traditional business organisation, market structure and contractual power relations. From a technological perspective it is mainly based on cloud computing power converted into economic tools, using algorithms;[1] from legal perspective, platforms impose their terms to all the users, without any room for negotiation and reduced ability of the traders to influence the rules of the game, by apportioning rights and establishing duties in equal manner.[2] Such process of mediation of relevant interests[3] is not necessarily performed in a clear and transparent manner[4]; very often the content of the contracts is not even really known to adhering users, who merely declare to have read and accepted them, by clicking a consent icon on their smartphone or tablet.[5] And in digital platform economy not only the conclusion of the contract changed, but also its execution, frequently done by algorithms,[6] where interaction between users is channelled within predetermined tracks, by limiting information the users can accede or exchange.[7] In terms of responsible business conduct an important issue is how narratives spread on social media platforms, having a great impact on how an individual may search for and encounter information. Individuals may be in fact subjected to discrimination, or have their personal data and privacy restricted. A good example is provided by the so-called "Twitter Files" that, in the interpretation provided by Elon Musk and some journalists, would prove that Twitter intentionally censored the U.S. conservatives because of their political views, invoking shadow banning. Probably an

[1] Martin Kenney and John Zysman, 'The rise of the platform economy' (2016) 32(3) Issues in science and technology 61.
[2] Christoph Busch, 'European Model Rules for Online Intermediary Platforms' in Uwe Blaurock, Martin Schmidt-Kessel and Katharina Erler (eds), *Plattformen Geschäftsmodelle und Verträge* (Nomos 2018) 37.
[3] Christoph Busch and others 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2016) 5 Journal of European Consumer and Market Law 164.
[4] Under the newly enacted EU Digital Services Act platforms' terms have now to be presented in a clear and concise manner and to respect users' fundamental rights.
[5] Donato Cutolo and Martin Kenney, 'Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy' (2019) Berkeley Roundtable on the International Economy Working Paper 3/2019.
[6] Gizem Alper, 'Contract law revisited: algorithmic pricing and the notion of contractual fairness' (2022) 47 Computer Law & Security Review (online); Maria José Schmidt-Kessen, Helen Eenmaa and Maya Mitre, 'Machines that Make and Keep Promises - Lessons for Contract Automation from Algorithmic Trading on Financial Markets' (2022) 46 Computer Law and Security Review.
[7] Sangeet Paul Choudary, Marshall W Van Alstyne and Geoffrey G Parker, *Platform revolution: How networked markets are transforming the economy and how to make them work for you* (W W Norton & Company 2016).

exaggeration, that in all events confirm the messy business of policing a large social network, that some commenter presented as part of an ongoing battle to control the narrative about democracy in America.[8] The challenge with figuring out the right regulatory response to social media platforms like Twitter and Facebook results from their dual role as public and private spheres. And the Twitter Files provided evidence of lack of transparency in social media, with growing concerns regarding dishonest data collection and users' privacy, which caused some social media platforms to implement explanatory tools to properly inform and empower consumers.[9]

More broadly, Big Techs governing digital online platform are "reorganizing the geography of how value is created, who captures it, and where",[10] by acquiring a great and frequently underestimated power.[11] In such a context risk of imbalance to the detriment of users is even higher,[12] and for those who are not prepared to accept said rules the only practicable exit strategy is to abandon the platform itself. In some cases dominant position could enable platforms to commit abuses against business users, and for such a reason the EU has published Regulation (EU) 2019/1150,[13] which provides for a more transparent and fair environment for business users that make use of digital platform services and, more generally - together with EU rules on copyright and geo-blocking - it's intended to protect consumers and, at the same time, to make European corporations more competitive in respect to the U.S. big market players.

In a marketplace governed by obscure algorithms public control is difficult and self-regulation is of essence; for such a reason the platforms, being virtual marketplaces, have strong interest in reducing risks and guaranteeing a safe market.[14] Insofar contracts are concluded in a condition of unequal contractual power to the advantage of the platforms, these disparities should be countered, at least to safeguard users' fundamental rights, by considering that in such an environment self-regulation becomes crucial. These fundamental rights are first represented by those enumerated in the Universal Declaration of Human Rights,[15] starting from rights to privacy, life and personal security, work, non-discrimination and freedom of opinion and expression. In fact, OECD works together with

[8] Micah Sifry, 'Putting the 'Twitter Files' in Perspective' (Medium, 16 December 2022) <https://micahsifry.medium.com/putting-the-twitter-files-in-perspective-f94756b051e5> accessed 19 March 2023.
[9] Daricia Wilkinson and others, 'The Pursuit of Transparency and Control: A Classification of Ad Explanations in Social Media' [2021] Proceedings of the 54th Hawaii International Conference on System Sciences 763.
[10] Mark Huberty, 'Awaiting the second big data revolution: From digital noise to value creation' (2015) 15(1) Journal of Industry, Competition and Trade 35.
[11] Matthew Zook and Taylor Shelton, 'Internet and global capitalism' in Douglas Richardson and others (eds), *The International Encyclopedia of Geography: People, the Earth, Environment and Technology* (John Wiley & Sons Ltd 2017) 11.
[12] Martin Kenney and John Zysman, 'The Platform Economy and Geography: Restructuring the Space of Capitalist Accumulation' (2020) 13(1) Cambridge Journal of Regions, Economy and Society 55.
[13] European Parliament and Council Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186, 57.
[14] José van Dijck, Thomas Poella and Martijn de Waal, *The platform society: Public values in a connective world* (OUP 2018).
[15] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

governments and citizens to establish evidence-based due diligence international standards for ensuring responsible business conduct, find solutions to economic, social and environmental challenges and build better policies that implement ethical AI principles, with the aim of fostering prosperity, equality, opportunity and well-being worldwide.[16]

More specifically:

- AI has the potential to benefit people and the planet by driving inclusive growth, sustainable development and well-being. Relevant commitments must be incorporated in product's design, sale, and use;
- AI systems' structure must comply with rule of law and respect human rights, democratic values and diversity;
- companies should be transparent and ensure that people understand AI-based outcomes/can challenge them;
- AI systems must function in a robust, secure and safe way. Companies should identify adverse impacts and take steps to mitigate, prevent and address them in their development, sale, and use;
- companies should be accountable and publicly report on due diligence efforts on a periodic basis;
- companies should provide for or cooperate with remediation mechanisms, if appropriate.

In terms of soft law also the UN Guiding Principles on Business and Human Rights[17] provide for standards of due diligence, transparency and remediation that companies should implement across their polices, practices, and products, so that they can be held accountable in terms of human rights impact.

Big Techs like Meta,[18] Microsoft,[19]and Intel[20] have conducted independent human rights impact assessments on their platforms. All these platforms have strong interest in reducing risks and guaranteeing safe transactions: for such a reason the U.S. legal system - used to facilitate running business with no overruling approach - adopted a sort of "*laissez faire*" approach, with Big Techs dominating the virtual marketplaces on the Internet. The European approach, on the contrary, is aimed at regulating digital markets and AI, on which relevant transactions are based.

[16] OECD responsible business conduct and human rights <https://www.oecd.org/industry/inv/responsible-business-conduct-and-human-rights.htm> accessed 19 March 2023.

[17] United Nations Guiding Principles on Business and Human Rights <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 19 March 2023.

[18] Miranda Sissons and Iain Levine, 'Meta's First Annual Human Rights Report' (14 July 2022) <https://about.fb.com/news/2022/07/first-annual-human-rights-report/> accessed 19 March 2023.

[19] Microsoft Global Human Rights Statement <https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement?activetab=pivot_1%3aprimaryr5> accessed 19 March 2023.

[20] Intel Global Human Rights Principles <https://www.intel.com/content/www/us/en/policy/policy-human-rights.html> accessed 19 March 2023.

1.1 EU regulations imposing transparency and due diligence obligations for online platforms

Online platforms base their business model on the collection and analysis of user data. AI systems work by ingesting large amounts of data, classifying it, analysing it for correlations and patterns and using these patterns to make predictions. This leads to the amplification of risks of infringing fundamental rights[21], especially when online platforms use AI systems[22] .

European Union legal framework for the protection of users' fundamental rights can be summarised as follows:

A) The General Data Protection Regulation EU 2016/679[23] (GDPR) protects individuals when their data is being processed by the private sector and most of the public sector.[24] The processing of data by the relevant authorities for law-enforcement purposes is subject to the Directive 2016/680.[25] Moreover, Regulation (EU) 2018/1725[26] protects natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, by upholding individual's fundamental rights and freedoms, especially the right to protection of personal data and the right to privacy and aligning the rules for EU institutions, bodies, offices and agencies with those of the GDPR and of Directive (EU) 2016/680.

In Italy processing data through a digital platform with algorithms has been already object of regulatory and courts' decisions, too, namely attaining use and access to digital platforms organising bike riders' food delivery:

- on 10 June 2021 Italian Privacy Authority[27] imposed a 2.6 million EUR fine on Foodinho, for not having informed its employees on the functioning of the

[21] Paul C Godfrey, Craig B Merrill and Jared M Hansen, 'The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis' (2019) 30(4) Strategic Management Journal 425.

[22] Sergio Román and Pedro J Cuestas, 'The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general internet expertise and word of mouth: A preliminary analysis' (2008) 83(4) Journal of Business Ethics 641.

[23] European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 1; see in particular Article 22.

[24] Edoardo Celeste and Giovanni De Gregorio, 'Digital Humanism: The Constitutional Message of the GDPR' (2022) 3(1) Global Privacy Law Review 4.

[25] European Parliament and Council Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119 89.

[26] European Parliament and Council Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, [2018] OJ L 295 39.

[27] Italian Data Protection Authority '*Ordinanza ingiunzione nei confronti di Foodinho s.r.l.*' (Italian Data Protection Authority, 10 June 2021) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9675440> accessed 19 March 2023.

system and for not having implemented suitable safeguards to ensure accuracy and fairness of the algorithmic results that were used to rate rider's performance. The platform had no procedures in place to enforce the right to obtain human intervention, to enable the employees to contest the decision taken by way of those algorithms which caused discrimination entailing the exclusion of some riders from work assignments;

- Court of Bologna[28] stated that use of the algorithm used by the platform to rate and organise the working timetable of the riders is discriminatory. In such a respect there were applied principles already stated in Italian Supreme Court Decision No. 1/2020[29], confirming that - in respect of labour cases only - also personal convictions of the workers, representing pragmatic profession of an ideology different from a religious one, don't legitimate difference in treatment of the workers in having access to the digital platform.

B) Specific resolutions regarding AI and RBC are represented by:

1) OECD Recommendations on artificial intelligence, adopted on May 22, 2019;[30]
2) European Union Commission White paper on AI, published on February 19, 2020;[31]
3) European Union Parliament Resolution on a framework of ethical aspects of AI, robotics and related technologies dated October 20, 2020;[32]
4) EU proposal for AI Regulation dated April 21, 2021,[33] intended to establish comprehensive regulatory scheme for development and use of AI, applicable to any provider of AI services in the EU market, particularly to those posing high risks.[34]

[28] *Filcams CGIL Bologna, NIDIL CGIL Bologna, FILT CGIL Bologna v. Deliveroo Italia s.r.l* [2020] Court of Bologna, Italy, ruling 31 December 2020 (case n. r.g. 2949/2019) <https://www.bollettinoadapt.it/wp-content/uploads/2021/01/Ordinanza-Bologna.pdf> accessed 19 March 2023.

[29] Italian Supreme Court, Judgement n. 1/2020, <https://www.wikilabour.it/wp-content/uploads/2021/02/Cassazione_2020_00001.pdf> accessed 19 March 2023.

[30] OECD Recommendations on artificial intelligence (22 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 19 March 2023.

[31] European Commission (EU) White Paper on Artificial Intelligence: a European approach to excellence and trust, COM/2020/65 [2020] <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 19 March 2023.

[32] European Parliament (EU) Resolution of 20 October 2020, with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, [2021] OJ C 404 107 <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html> accessed 19 March 2023.

[33] European Commission (EU) 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts'[2021] COM/2021/206 <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence> accessed 19 March 2023, and relevant explanatory report <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 19 March 2023.

[34] European Commission (EU) Explanatory Memorandum to COM[2021)21 - Amendment of Directive 2014/41/EU, as regards its alignment with EU rules on the protection of personal data, SEC[2021] 167 <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence> accessed 19 March 2023.

C) The so-called EU Digital Package, structured by:

1) Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services, amending Directive 2000/31/EC, better known as Digital Services Act or DSA,[35] based on the Proposal for a regulation for digital services dated 15 December 2020[36] and providing for certain very large online platforms' obligations. They could be summarised as follows:
   (i) appointment of internal compliance officers;
   (ii) duty to mitigate risks;
   (iii) risk assessment, including the risks of dissemination of illegal content through their online services and potential negative effects for privacy and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child;
   (iv) independent audit once a year to assess compliance;
   (v) additional online advertising transparency.

   Violations of the DSA may result in penalties of up to 6% of total worldwide annual turnover, so exceeding penalties provided under the GDPR.
   DSA introduced the right as well to compensation for damage or loss suffered by users due to a provider having violated its obligations under the DSA.
2) EU Regulation 2022/1925, on contestable and fair markets in the digital sector, usually known as *Digital Markets Act* or DMA,[37] adopted on 14 September 2022 and based on the Proposal for a Regulation for markets in the digital sector dated 15 December 2020[38] . The Digital Markets Act is a regulatory response to the perceived inability of competition law (and the prohibition to abuse a dominant position as per Article 102 TFEU) to tackle specific types of behaviour of Big Tech companies.

It will apply to the so-called "gatekeepers", i.e. core platform services like:
   (i) online search engines like Google;
   (ii) online intermediation services like Amazon;
   (iii) online social networking services like Facebook;
   (iv) video-sharing platform services like YouTube,

[35] European Parliament and Council Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), [2022] OJ L 277, 1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065> accessed 19 March 2023.
[36] European Commission (EU) Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 [2020] <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN> accessed 19 March 2023; Alexander Peukert and others, 'European Copyright Society – Comment on Copyright and the Digital Services Act Proposal' (2022) 53 IIC 358.
[37] European Parliament and Council (EU) Regulation 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), [2022] OJ L 265 1 <https://eur-lex.europa.eu/eli/reg/2022/1925> accessed 19 March 2023.
[38] European Commission (EU) Proposal for a Regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 [2020] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN> accessed 19 March 2023.

and, also, to operating systems, web browsers, cloud computing services, virtual assistants, interpersonal communications services like WhatsApp, and any and all online advertising services provided by the above-mentioned gatekeepers, insofar these gatekeepers: (a) have a significant impact on the EU market; (b) represent an important gateway for business users to reach end users and (c) enjoy an entrenched and durable position or it is foreseeable that they will enjoy such a position in the near future. For each of these qualitative criteria, the Digital Markets Act provides certain quantitative thresholds that, if met, create a presumption that the qualitative criteria are met and give rise to an obligation to notify to the European Commission. The *Digital Markets Act* also provides for an anti-circumvention clause, prohibiting undertakings from segmenting, dividing, fragmenting or splitting its core platform services to circumvent the abovementioned quantitative thresholds. The European Commission shall be in charge of designating the gatekeepers by Autumn 2023 and to guarantee the application of the relevant rules and sanctions.

3) European declaration on digital rights published on 16 November 2022,[39] which aims to promote European values within the digital transformation, putting people at the centre, with digital technology benefiting all individuals, businesses, and society as a whole, based on the Proposal for a Declaration on Digital rights and Principles dated 26 January 2022.[40] Based on relevant principles large online platform should support free democratic debate online. They should mitigate the risks stemming from the functioning and use of their services, including for disinformation campaigns and protect freedom of expression.

   Core principles could be summarized as follows:

   (i) The system must be based on solidarity and inclusion, safety, security and empowerment of individuals, by ensuring freedom of choice online and participation to the digital public space;[41]

   (ii) Transparency is required in the use of algorithms and AI, so that people be properly informed when interacting with them;

   (iii) Algorithms and AI must not be used to pre-determine people choices;

[39] Council of the European Union (EU) Provisional agreement of Council of the EU and European Parliament on European declaration on digital rights and principles <https://www.consilium.europa.eu/en/press/press-releases/2022/11/14/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/> accessed 19 March 2023.

[40] European Parliament (EU) European Declaration on Digital Rights and Principles for the Digital Decade, Brussels, 26.1.2022 COM [2022] 28 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733518/EPRS_BRI[2022)733518_EN.pdf> accessed 19 March 2023.

[41] Alec Tarkowski and Paul Keller, 'Digital Public Space - A Missing Policy Frame for Shaping Europe's Digital Future' in Alexander Baratsits (Ed) *European Public Spheres, Digitization and Public Welfare Orientation* (iRights 2021).

(iv) Algorithms must avoid unlawful discrimination and enable human supervision;
(v) children rights protection must be guaranteed. Children and young people in general should be empowered to make safe and informed choices and express their creativity in the online environment.

Moreover, national regulations about internet services exist in certain European countries, like in Germany, where existing applicable regulations have been supplemented with the Network Enforcement Law (NetzDG),[42] which requires companies to remove unlawful content and provides for substantial penalties where they fail to do so.

1.2 Safeguard of fundamental rights and new frontiers of drug-device technologies: how to combine relevant human rights and interests?

A last frontier for testing RBC principles is represented by digital pills (DP), an innovative drug-device technology that permits to combine traditional medications with a monitoring system that automatically records data about medication adherence as well as patients' physiological data. The pill chip can send information from inside the patient's body to a patch that is placed on the patient that sends the information to a smartphone app that can be accessed by doctors, patient, caregivers. It is foreseeable that many other traditional medications will be digitalised to allow a reliable monitoring of medication-taking behaviour and the collection of data concerning the patients. DPs, being regarded as pharmaceutical or medical devices, needs Marketing Authorisation Approval from regulatory bodies before assessing the market.[43] The European Medicines Agency – EMA has recognised DP "as a qualified method for measuring adherence in clinical trials". At the end of 2017, the first DP combined with a traditional drug was granted market approval as a medication by the U.S. Food and Drug Administration (FDA).[44]

That has significant benefits:

- improving the quality and cost of care for the millions of people suffering from uncontrolled illness;
- improving the communication and the counselling interventions of healthcare providers to the possibility of transmitting real-time reliable data about patients and their health-related behaviour

But pose some significant open questions:

[42] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Federal Law Gazette I, 3352 ff., 1 October 2017) <https://germanlawarchive.iuscomp.org/?p=1245> accessed 19 March 2023.
[43] Andrea Martani and others 'Digital pills: a scoping review of the empirical literature and analysis of the ethical aspects' (2020) 21(3) BMC Med Ethics.
[44] FDA decision for approval DP (ariprazole drug) states that: "if the (...) system fails, patients will not incur additional risk; they will continue to receive the exact treatment benefits of aripiprazole tablets without tracking. If the system works as intended and the patient chooses to share the data with the HCP [health care providers], the drug ingestion data could potentially help guide the prescribing physician on treatment interventions".

- do DPs meet the legal definition of pharmaceutical or medical device is a real challenge?[45] In fact, legal qualification of new health technologies is a hard issue. It confronts sometimes a total legal vacuum;
- long-term adverse effects and issues regarding product shelf-life are currently unknown, like possible adverse effects or drug interaction reactions;
- long term use issues such as efficacy and maintenance are as well questionable;
- reimbursement system can impact the political and economic strategies for integrating innovation.

And, even more, by introducing DPs are we swallowing a spy, which might affect individuals' autonomy, representing an unpleasant form of surveillance and even impacting on doctor-patient relationship?[46]

The unknown risks of digital medicines solutions lead to the mobilisation of legal norms that govern acts and activities, as well as the construction of jurisprudence to guide the balance between risks and benefits. Thinking about the security, safety, lifecycle and privacy concerns in e-health is crucial; nevertheless, principle of precaution cannot prevent the advancement of technology due to the lack of knowledge of the risk. An up-to-date legal control of the risk-benefit binomial is so required, to avoid the maximum damage from health problems due to new digital health therapies.[47]

2 Metaverse and RBC: what perspective for the safeguard of online users' fundamental rights?

Meta is Greek for "beyond". With historic roots in science fiction, it was first defined in this 1999 book as a virtual universe controlled and owned by a "global information monopoly that users can access via personal VR goggles."[48] The Metaverse is now in its infancy but promises to soon become the internet of the future! There is currently no truly united place for the Metaverse to be experienced. Numerous virtual worlds exist, and technology is beginning to bring together virtual content which never existed before[49] and

[45] The European Court of Justice has been required by the *French Conseil d'État* to assess whether a software - with at least one function that makes it possible to use patient-specific data for the purposes, inter alia, of detecting contraindications, drug interactions and excessive doses - has to be classified as a medical device under the EEC Medical Device Directive 93/42. With ruling C-329/16 ('*Snitem v. Syndicat national de l'industrie des technologies médicales*', published on 7 December 2017) the European Court of Justice ruled that a software constitutes a medical device for the purposes of the EE Directive 93/42 (now replaced by the EU Medical Device Regulation 745/2017), insofar it satisfies the two cumulative conditions – which must be met by any device of that nature – relating to: (i) the objective pursued and (ii) the action resulting therefrom.

[46] Lauren M Wancata and Daniel B Hinshaw, 'Rethinking autonomy: decision making between patient and surgeon in advanced illnesses' (2016) 4(4) Ann Transl Med 77.

[47] Gualberto Gussoni, 'Digital Therapeutics: an opportunity for Italy, and beyond' (2021) 4 Tendenze nuove 3.

[48] Neal Stephenson, *Snow Crash* (Random House Publishing Group 1992).

[49] Liang-Jie Zhang, 'MRA: Metaverse Reference Architecture' in Bedir Tekinerdogan, Yingwei Wang, Liang-Jie Zhang (eds.) *Internet of Things - ICIOT 2021*, (Springer International Publishing AG 2021).

creating legal challenges never before imagined[50]. The goal is for the Metaverse to embody the evolution of the Internet into "a single, universal and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets."[51] It must be intended in a wider meaning, including all possible interactions of the user in a digital or hybrid environment, combining a digital lawyer with physical reality. Interfaces can also include body armour, to help one feel totally immersed in the experience: in such a manner the Metaverse promises to bring the virtual world to life. And from a technical perspective it shall represent just a sort of natural evolution from an Internet 1.0, in which we were just able to share contents, passing through an Internet 2.0 where we can pass from a passive role to an interaction which the exchanged contents. Metaverses could grow into entire societies with economies and democratic leadership. And Metaverse is by sure a big business, made of corporate metaverses, seeking to maximize monetary transactions.[52][53]

In such a new virtual reality many companies have already found creative and fruitful ways to use the Metaverse as a marketplace and to make transaction safer by trading Non-Fungible Tokens (NFTs). They are unique cryptographic tokens recorded and minted on a cryptocurrency's blockchain; they cannot be replicated, because they are assigned unique identification codes and metadata that distinguish them from other tokens.[54] Because every NFT is unique, tokens are coded to prove ownership of user-generated content and NFT assets; that represents a real-world economic value, insofar holders of crypto tokens, avatar skins, and digital real estate can trade them, giving them real-world value.[55]

Metaverse reality and relevant use of NFTs and cryptocurrencies - together with underlying policies and regulations, risks and opportunities - represent an extremely actual and controversial subject in all jurisdictions and economies worldwide. A subject largely discussed in Parliaments and in courts and which is becoming more and more of interest for various industries, for preserving and safeguarding existing assets and looking for future business opportunities in another promising market dimension. Metaverse is in fact expected to deeply influence the real world and this influence impact particularly

[50] Yogesh K Dwivedi and others, 'Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy' (2022) 66 International Journal of Information Management.
[51] Matt O'Brian and Kelvin Chan, 'EXPLAINER: What is the metaverse and how will it work?' (Los Angeles Times, 28 October 2021) <https://www.latimes.com/business/story/2021-10-28/explainer-what-is-the-metaverse-and-how-will-it-work> accessed 19 March 2023.
[52] In January 2022 Microsoft, which owns the Xbox video game console system, declared its intention to acquire Activision Blizzard Inc. for US$68,7 billion, which would make it the biggest gaming industry deal in history, to play a key role in the development of metaverse platforms. Activision is the maker of popular games including Call of Duty and World of Warcraft. But in December 2022 the US Federal Trade Commission has moved to block Microsoft's takeover, citing concerns that the deal would thwart competition, by denying rivals access to popular gaming content.
[53] Facebook renames 'Meta' and commits US$180 billion to develop metaverse. Mark Zuckerberg said it's a 'reasonable construct' for the metaverse to be a time, not a place.
[54] Jimmi Aky, 'Guide to tokens and NFTs: what is 'tokenization' and how does it work?' *Forkast News* (9 March 2021) <https://forkast.news/tokens-nfts-tokenization/> accessed 19 March 2023.
[55] Samuel J Bolton and Joseph R Cora 'Virtual Equivalents of Real Objects (VEROs): A type of non-fungible token (NFT) that can help fund the 3D digitization of natural history collections' (2021) 6(2) Megataxa 93.

the luxury sector, by allowing multiple industries to enhance their brands and expand their business. However, the Metaverse is not a uniform entity, but a broad term applied to a range of virtual experiences. There are various platforms providers within it, some of which are owned by a single legal entity, and others run by decentralised autonomous organisations (DAOs). With blockchain technology, ownership of the metaverse is shared by its users, and DAOs put users in control of the game's future. The incoming Metaverse dimensions under establishment offer room enough for fixing appropriate rules of engagement between digital platforms on one side and private and professional users on the other side, for the benefit of end users worldwide. That, even if Metaverse, from a users' perspective, is still a matter for pioneers only, looking to the pretty low number of active users logged for instance in The Sandbox Game or in Decentraland.[56]

That shall surely require the adoption of specific regulations for digital assets and cryptocurrencies, as China already did, launching its first state backed NFT marketplace and allowing from 1 January 2023 their free trading, insofar they are kept into a wallet integrated into a digital platform named China Digital Asset Trading Platform and run – having obtained a compliance license through China Technology Exchange - by three state-owned and private entities, namely including China Technology Exchange and Art Exhibitions China, both of which are government-backed, and Huban Digital, a private company. The marketplace is built on "Wenbao Chain" (China Cultural Protection Chain), a blockchain network operated by Art Exhibition China, and will also be used to trade digital copyrights and property rights along with collectibles. And in November 2022 the Hangzhou Internet Court ruled that digital assets have similar property rights to items sold on e-commerce sites.[57]

These regulations become even more necessary after the many frauds recently occurred, starting from the Markets in Crypto-Assets (MiCA) Regulation,[58] intended to establish a harmonised set of rules for crypto-assets and related activities and services and to impose restrictions on the issuance and use of stablecoins, expected to enter into force in early 2023. Mica is part of a digital finance package, which, inter alia, also includes the Digital Operational Resilience Act[59] and the DLT Pilot Regime Regulation,[60] based on distributed ledger technology, which itself will start applying on 23 March 2023. The regime is a regulatory sandbox for facilitating the development of secondary market

[56] Stefan M, 'How Many Active Users Does Decentraland Really Have?' (Nftnewstoday, 18 October 2022) <https://nftnewstoday.com/2022/10/18/how-many-active-decentraland-users/> accessed 19 March 2023.

[57] Hangzhou Internet Court '拼手速抢购的"NFT数字藏品盲盒"被退款，买家索赔9万余元，法院判了 (*The "NFT Digital Collection Blind Box" that was snapped up quickly was refunded, and the buyer claimed more than 90,000 yuan, and the court ruled*) <https://mp.weixin.qq.com/s/WWnZAxqiIVJ-dHO90eoBVw > accessed 19 March 2023.

[58] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)' COM/2020/593 final 24 September 2020.

[59] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014' COM(2020) 595 final, 24 September 2020.

[60] European Parliament, 'Proposal for a Regulation of the European Parliament and of the Council on a Pilot regime for market infrastructures based on distributed ledger technology' COM/2020/594 final, 24 September 2020.

infrastructure for digital securities, including both "tokenised" securities and digitally native securities.

The key questions are: how responsible business conducts shall be ensured in the Metaverse? Who will regulate this unsettled digital technology? That even more looking to recent EU rules for the digital market, which could imply a substantial change in applicable regulatory framework.

In the European Union regulations that apply to two-dimensional social media platforms also apply to the metaverse itself and the services offered therein. That even if the Digital Services Act does not specifically mention either Metaverse or virtual reality, and in 2021 the EU Commission stated that it wanted to refrain for the time being from creating any regulations for the metaverse launched by Meta Group. But additionally, we will have to consider all the offences, having sometimes also criminal relevance, which could concern our avatar when moving inside the Metaverse dimension.

RBC is expected to evolve also at Metaverse level, and the potential benefits of Metaverse will arise only insofar issues around its ethical and accountable use are effectively resolve,[61] with an AI systems' structure that must comply with rule of law and respect human rights, democratic values and diversity. That means to incorporate relevant commitments in the design of this new virtual dimension and of relevant products' design, sale and use and, more generally, to allow sustainable development. Basic requirements are that AI systems must function in a robust, secure and safe way and companies dealing online ensure that people fully understand AI-based outcomes and may challenge them, if required; and the general cybersecurity and data protection risks on the internet obviously also apply. Platforms are so required to identify adverse impacts and take steps to mitigate, prevent and address them.

Platforms are so expected to be more and more transparent and accountable, by publicly reporting on their due diligence efforts and providing for appropriate remediation mechanisms, if appropriate. Big Techs like Meta, Microsoft and Intel are periodically conducting independent human rights impact assessments on their platforms and a similar effort shall be even more required in a context of virtual and augmented reality like Metaverse, in terms of respect and true enforcement of applicable rights and regulations.

Far from being a mere gadget for gamers only, according to technology research firm Gartner, by 2026 one out of four individuals worldwide is expected to spend at least one hour a day in the Metaverse to work, study, shop and socialize[62]. The new technologies have the potential to bring positive impact and effects in various key areas, like life sciences, medicine and educations, and these are the reasons for massive investments by Big Tech in recent years. But these entities must be the first to ensure that profits are not

[61] Muhammad Anshari and others, 'Ethical Responsibility and Sustainability (ERS) Development in a Metaverse Business Model' (2022) 14(23) Sustainability (n. 15805).
[62] Pankaj Prasad, Padraig Byrne and Gregg Siegfried 'Market Guide for AIOps Platforms' (Gartner, 30 May 2022) <https://www.ibm.com/downloads/cas/AXO20DXM> accessed 19 March 2023.

put before legitimate users' interest, namely avoiding massive data collection and their improper use, in a global scenario where also crime is gradually moving digital. If the borders of our real world are melting into the digital universe, there is an emerging need of protecting citizens and ensuring the rule of law also in this new dimension.

The question is if, in the on-going Metaverse development, self-regulation and ethical guidelines and standards could really represent safeguard enough against bad and improper use of AI, where fundamental human rights are and must remain central. And where the International Principles on the Application of Human Rights to Communications Surveillance must be constantly adjourned and even more enacted, so that users' data are treated in the legitimate interest of their proprietary owners and for the benefit of the community, by avoiding and sanctioning any sort of manipulation or harm. That represents a new test field for the legal community everywhere in the world, not only in terms of enacting new laws and regulations and adopting smart contracts, but also in terms of law enforcement, where the Metaverse could provide many benefits, including telecommuting, matchmaking, collection and preservation of crime scene evidence. That was recently shown at INTERPOL's 90th General Assembly in New Delhi, where the global police organization unveiled the first-ever Metaverse specifically designed for law enforcement agencies around the world, allowing registered users to receive immersive training in forensic investigations and other policing capabilities.[63]

In the United States they adopted a pragmatic approach in ensuring Responsible Business Conduct, articulated into:

- recourse to smart contracts, represented by programmed digital codes that run on the blockchain,[64] automate operations, and ensure that trading and transactions are done according to the predetermined rules. They are not legally binding contracts, but a mere set of rules that control the use of specific NFTs,[65] and later purchasers may not realise that a smart contract does not necessarily provide same benefits as it did to original owner. They can be programmed to automatically pay royalties, buy and sell NFTs, make donations and more, by granting speed and efficiency: no paperwork to process required. Moreover, trust and transparency are ensured, being they hard to hack. But these systems are not infallible: crash and mistakes in coding are still made;[66]
- technology solutions: for instance, due to allegations of asserted harassment, Meta now gives all virtual reality ("VR") participants a two-foot 'personal boundary' by default, blocking wayward hands from drawing too close. The force

[63] INTERPOL 'INTERPOL launches first global police Metaverse' (INTERPOL, 20 October 2022) <https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse> accessed 19 March 2023.
[64] Riccardo de Caria, 'Definitions of Smart Contracts: Between Law and Code' in Larry DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (CUP 2019) 19.
[65] Peter G L Hunn, 'Smart Contracts as Techno-Legal Regulation (2019) 7(3) Journal of ICT Standardization 269.
[66] James Grimmelmann, 'All Smart Contracts are ambiguous' (2019) 2(1) Journal of law and innovation 2.

field-style safety mechanism has been rolled out across Meta platforms, limiting interactions between avatars, and creating an invisible virtual barrier all around, preventing other people from getting too close;[67]

- crypto tokens (like ERC-20) built into existing blockchains as corporate governance mechanism.[68] Some crypto tokens represent tangible assets such as real estate or art and others represent intangible assets such as governance voting rights on the platform. In decentralised platforms, crypto tokens can also be used as a governance mechanism for decisions that dictate future direction of various blockchain projects. Decentralised governance is still evolving, but key processes are being standardised and implemented so that protocols can be equitably enforced. No such self-governance is promised, for the time being,[69] under corporate Metaverse (such as Microsoft or Meta/Facebook);
- licensing virtual goods. For instance, Nike filed multiple applications seeking U.S. trademark protection for virtual goods. The applications are on an intent-to-use basis, so they won't be finalised until they're in commercial use. The new trademarks provide Nike extra protection in the event others attempt to use the brand in an unlicensed way.

In the United States a huge challenge is represented by the fact that federal laws often defer to individual state laws, which are fractured and inconsistent. With no national privacy laws and pending a proposal for a Federal American Data Privacy and Protection Act,[70] the State of California is currently the gold standard on U.S. privacy laws. If passed, the Federal American Data Privacy Protection Act would limit data collection and allow for enforcement by the U.S. Federal Trade Commission, although, as it is currently written, it is more limited than California's privacy laws. Government regulators and court decisions shall have to rely on the applicable existing U.S. federal laws covering:

- Cybersecurity
- Antitrust
- Unfair trade practices
- Intellectual Property (trademarks, copyrights)
- Securities/Banking
- Gambling/ Lottery laws
- Currency
- Protection of Children and disabilities.

[67] Jan Mulligan, 'Metaverse: What Regulation? U.S. Laws… Regulation by Speculation' [2022] Mulligan Law - Blog <https://www.janmulligan.com/metaverse-what-regulation-u-s-laws-regulation-by-speculation/> accessed 29 March 2023.
[68] Philipp Hacker and others, 'Regulating blockchain: techno-social and legal challenges' (OUP 2019) 311.
[69] Melanie Swan, '*Blockchain. Blueprint For a New Economy*' (O'Reilly 2015).
[70] Introduced in Congress in June 2022, having Rep Frank Pallone Jr as sponsor, reported (amended) by the Committee on Energy and Commerce and placed by the House of Representatives on 30 December 2022 on the Union Calendar (Calendar 488) <https://www.congress.gov/congressional-report/117th-congress/house-report/669> accessed 19 March 2023.

Existing laws are in many respects inadequate for novel issues, such as the scope of the right to use content held by an NFT owner. New laws are needed, but U.S. federal regulators are usually slow, preferring to take a "wait and see" attitude. And there will be problem with enforcement because of lack of borders/jurisdiction in digital disputes.

Some U.S. states are considering enacting laws that regulate social media platforms and up to now Florida and Texas have passed such laws, by limiting the power of the largest social media platforms to moderate and curate speech and requiring those companies to disclose certain information to the public. Two trade organisations representing the social media companies challenged both laws, allegedly seeking protection under the U.S. Constitution guaranteeing freedom of speech. Federal district courts enjoined each law, holding that the companies were likely to succeed on their First Amendment challenges, and the cases were appealed.

The Florida law is known as the Stop Social Media Censorship Act. It was proposed shortly after former President Donald Trump, following the January 6 insurrection at the U.S. Capitol, was suspended from Twitter and other social-media platforms. Among other things, the law bars social-media platforms from banning political candidates and journalistic enterprises.[71] On 23 May 2022, in the *Moody v. NetChoice* case, the Eleventh Circuit struck down the part of the Florida law that limits the power of social media platforms to moderate and curate content but upheld the law's disclosure provisions[72]. The U.S. Court of Appeals for the 11th Circuit blocked Florida from enforcing most of the law's provisions, prompting the State to come to the Supreme Court in September 2022.

The Texas law is known as House Bill 20. It sought to prohibit social media companies from banning users over their viewpoints, even if their rhetoric was offensive or erroneous. The law also sought to require the corporations to explain and disclose reasons for any individual to be banned from the website, which would be cumbersome. If the Texas law was upheld, corporate governance over such issues is severely limited. In a close 5-4 decision, the High Court blocked the law from taking effect. However, that was only a temporary ruling that was overturned by the Supreme Court in May 2022. On appeal[73], NetChoice argued that prohibition on viewpoint-based censorship was unconstitutional, but the Fifth Circuit rejected these arguments, considering platforms as "common carriers". On the contrary, platforms argue they are more similar to newspapers. After the U.S. Court of Appeals for the 5th Circuit ruled for the State, the tech companies

[71] Sofia Andrade, 'Florida's New Pro-Disney, Anti-Facebook and Twitter Law' (Future Tense, 25 May 2021) <https://slate.com/technology/2021/05/florida-stop-social-media-censorship-act-disney.html> accessed 19 March 2023.

[72] *NetChoice, LLC v Attorney General, State of Florida* [2022] US District Court for the US Court of Appeals for the Eleventh Circuit) Opinion of the Court (May 23, 2022) <https://clearinghouse.net/doc/134778/> accessed 19 March 2023.

[73] *NetChoice, LLC v Ken Paxton*, in his official capacity as Attorney General of Texas Appeal from the United States District Court for the Western District of Texas [2022] U.S. Court of Appeals for the Fifth Circuit No. 21-51178, USDC No. 1:21-cv-840 https://www.ca5.uscourts.gov/opinions/pub/21/21-51178-CV1.pdf> accessed 19 March 2023.

returned to the Supreme Court in December 2022, asking the justices to take up their challenge. Texas Solicitor General Judd Stone agreed with NetChoice that review should be granted and urged the justices to consider both the Texas law and the Florida law at the same time. Rather than granting or denying review, the court opted to seek the views of the Biden administration. As a result, even if the justices ultimately decide to grant review, they almost certainly will not hear oral argument until next term, with a decision to follow sometime in 2024.[74] Until then, both States' laws will remain on hold and whether a social media platform's content moderation policies constitute speech protected by the First Amendment shall surely continue to carry serious implications for the future of online discourse.

3 Conclusions

Digital platforms are changing their skin, name, terms and conditions of access (not necessarily free of charge, even for socials) and sometimes even their ultimate owner, like already occurred for Twitter. Metaverse shall represent an unavoidable area of their expansion, not just for gaming applications, but even more for business purposes, through the recourse to NFTs and cryptocurrencies. In a proprietary virtual 3D space, a person will take the form of an avatar and move freely to do much of what one does in the "real" world: shop, take classes, attend meetings and concerts, exercise, compete in sporting activities, own virtual and physical assets, and make creative and financial investments that the individual can own, control and sell. Instead of looking at a screen, the feeling is to become part of connected virtual world. In such a context to delegate responsible business conducts of the digital platforms to self-regulation only shall be probably not enough. Platforms are so expected to be more and more transparent and accountable and applicable regulations are increasingly focusing on good faith efforts to protect centrality of fundamental human rights *vis-à-vis* Big Techs. Digital platforms shall have surely to implement and constantly improve robust and bullet proof procedures, insofar they do not want to be overwhelmed by class actions that would necessarily lead them not only to massive sanctions and loss of image, but even more could induce courts all over the world to cause them to disclose and make public their core assets, i.e. the algorithms representing the founding basis of their own business.

Responsible Business Conduct will no longer be for digital platforms operating in that 3D environment a mere nice to have, and a true self-government of the platforms shall necessarily require clear and effective regulations, enforceable not only within our European Union boundaries, but also in common law jurisdictions.

[74] Amy Howe, 'Justices request federal government's views on Texas and Florida social-media laws' (23 January 2023) <https://www.scotusblog.com/2023/01/justices-request-federal-governments-views-on-texas-and-florida-social-media-laws/>.

Therefore, the Metaverse represents a great opportunity, also from a regulatory perspective, by allowing to relevant jurisdictions to play no longer the role of followers in remedying lack of transparency for social media and online services, and in anticipating at their outset the occurrence of all the "improper occurrences" that have characterised the Internet and 2D age. That namely includes violation of privacy, unauthorised transfer of personal data to third parties and other conducts that could facilitate ID thefts, discrimination among the users, shadow banning and account freezing. It would be a serious mistake to think that the Metaverse is just an invention or a passing trend and not a logical evolutionary stage of our digital interaction with third parties. And States and Parliaments should not lose the opportunity to regulate risks and opportunities that the Metaverse and relevant communication and trading tools will unavoidably entail.

Fatih Buğra Erdem[*]

IS IMPEDING INNOVATION ANTICOMPETITIVE?

Abstract
This article considers innovation from the standpoint of contemporary EU competition law, by investigating whether and to what extent it protects the spread of innovation and conceptualising the anti-competitive characteristics of practices impeding innovation.

JEL CLASSIFICATION: K10; K21

SUMMARY

1 Introduction: fundamental theories of us antitrust law and the *sui generis* form of EU competition law

When EU competition law was established by the Rome Treaty in 1957, US Antitrust law had already moved forward by the implementation of the Sherman Antitrust Act in 1890. Hence, there seems little doubt that a study focusing on EU competition law will presumably fall short if the theories of US Antitrust law are not questioned even to a small extent. Besides, it is almost certain that competition law and economics are an integral part of a system as economic thinking has exerted an influence over the foundation of competition law. Therefore, this preliminary remark necessarily proceeds to encapsulate basic socio-economic justifications of US Antitrust law before it demonstrates the foundation of EU competition law together with its controlling idea behind to estimate aims and objectives. Last, it argues the practicability of this law in whether it ensures the necessary safety of the progression of innovation.

[*] Ph.D; Lecturer, Social Sciences University of Ankara, fatihbugra.erdem@asbu.edu.tr.

As regards the wide-ranging discussions while the foundations of US Antitrust law were laid, one may simply observe that every discussion leads to an economic controversy. While industrial policy advocates had the opinion that antitrust policies will improve social welfare only if they sustain large industrial organisations,[1] the critical legal studies movement presented by Unger, Fox and Sullivan merely underlined that the application of antitrust is of no use in terms of the welfare of people, but it legitimises the capitalist (monopolistic) exploitation.[2] However, the sharpest, long-standing, and continuing debate started between Harvard and Chicago schools' intellectual movements. Bain, Turner, Mason and others from Harvard school made no compromises over the discussion of 'structure-conduct-performance' regarding their position against the centralisation of capital.[3] They consequently emphasised the necessity of market intervention with respect to several criteria such as price flexibility, development of new technologies and market entry conditions. The Chicago School objected to this interventionist-inclined phenomenon because it did not coincide with the American dominant economic thought of neoliberalism, which reached its apogee in Reagan's time.

The elementary idea of the Chicago School is to maximise productive efficiency to increase public wealth.[4] This is why per se prohibitions of the Court without ratiocinating the effects of practices on consumer welfare are required to be extinguished. For instance, they took this assertion much further with the seemingly contestable argument that monopolies and concentrations may provide much more efficiencies.[5] According to Bork, unless the practice increases the cost of consumption (immediate cost), legal intervention would be required.[6] Scholars from the Chicago School, namely Coase, Director, and Posner, also established the relationship between law and welfare economics by demonstrating the canons of pareto-optimal equilibrium.[7] The major pillar of this Pareto efficiency is to achieve social welfare (socially optimal outcome) with the help of competitive markets (limited market intervention). Bork subsequently formed a basis for the concept of welfare in practice on top of this burgeoning literature.[8] However, it should be noted that this welfare concept is different from European understanding.

It is generally acknowledged that this is not all that Antitrust has affected with other doctrines, such as populist and post-Chicago.[9] Such aspects, as well as the

[1] David Audretsch, 'Industrial Policy and Industrial Organization' in Dennis Mueller, Alfred Haid and Jürgen Neumann (eds), *Competition, Efficiency, and Welfare* (Springer 1991) 223.
[2] Roberto Unger, '*The Critical Legal Studies Movement*' (Verso 2015); Eleanor Fox and Lawrence A. Sullivan, 'Antitrust-Retrospective and Prospective: Where are we coming from? Where are we going?' (1987) 62 New York University Law Review 936, 961-964.
[3] Paul Ferguson, *Industrial Economics: Issues and Perspectives* (Macmillan Education 1988) 7-22.
[4] Richard Posner, 'The Chicago School of Antitrust Analysis' (1979) 127 University of Pennsylvania Law Review 925.
[5] Richard Posner, *Antitrust Law* (The University of Chicago Press 2001); Herbert Hovenkamp, *The Antitrust Enterprise: Principle and Execution* (Harvard University Press 2005).
[6] A requirement imposed by law for the validity of a legal transaction.
[7] Jules Coleman, 'Efficiency, Utility, and Wealth Maximization' (1980) 8 Hofstra Law Review 508; See also, Posner (n 4).
[8] Robert Bork, *The Antitrust Paradox* (The Free Press 1993).
[9] Robert Atkinson and David Audretsch, 'Economic Doctrines and Approaches to Antitrust' (The Information Technology and Innovation Foundation, 2011) 1-33 <https://www2.itif.org/2011-antitrust.pdf> accessed 14 March 2023.

abovementioned ones, have aroused curiosity concerning different perspectives of welfare. Pittman measured welfare by using the deadweight loss, which addresses the difference between the appraised value of consumers and requested reasonable value by manufacturers.[10] In reference to the distribution of this amount, scholars have not arrived at a consensus yet. While some argue competition law aims to maximise total welfare (total surplus of society including both consumers and producers),[11] others defend the principle of maximising consumer welfare (benefit of consumers based on their consumption).[12] In conclusion, the enforcement of competition rules today took its final form in the US based on not only this debate but also untold other discussions. Even if, EU competition law shows similarities with US Antitrust law and its economic theories to some extent, it has a sui generis structure.

The fundamental aim of EU competition law is to provide free and undistorted competition to make the internal market more competitive for the sake of consumers and the better functioning of the internal market.[13] The CJEU verified this in the Continental Can case that competition law does not only consider direct damages to consumers, it also undertakes other anti-competitive conduct having direct or indirect effects on the market.[14] Therefore, the impact area of EU competition law, particularly Article 102 TFEU's scope of application, consistently enlarges[15] in accordance with the everchanging political and economic objectives of the EU and the values of European societies.[16]

The protection and operability of the European common market is the distinctive target of EU competition policy.[17] Since this special characteristic requires a one-size-fits-all approach, it precisely corresponds to the theory of ordo-liberalism developed by Freiburg School in the process of harmonising the economic interests of Member States.[18] It is more

[10] Russell Pittman, 'Consumer Surplus as the Appropriate Standard for Antitrust Enforcement' (2007) 3(2) Competition Policy International 205.
[11] ibid; Joanna Goyder and Albertina Albors-Llorens, *EC Competition Law* (OUP 2009); Ken Heyer, 'Welfare Standards and Merger Analysis: Why not the best?' (2006) 2(2) Competition Policy International 29.
[12] Pursuant to Massimo Motta, *Competition Policy and Practice* (CUP 2004), who served to EC as a chief economist, both approaches give approximately same results. Also see, Damien Neven and Lars-Hendrik Röller, 'Consumer surplus vs. welfare standard in a political economy model of merger control' (2005) 23 International Journal of Industrial Organisations 829; Sven-Olof Fridolfsson, 'A Consumer Surplus Defense in Merger Control' in Vivek Ghosal and John Stennek (eds), *The Political Economy of Antitrust* (Emerald Publishing 2007).
[13] Article 3/1(b) of TFEU. See also, Case C-52/09 *Konkurrensverket v TeliaSonera Sverige AB* [2011], paras 20-21.
[14] Case 6/72 *Continental Can Company Inc. v Commission of the European Communities* [1973], para 26. This is also stated in the Commission's enforcement priorities with regard to the use of Article 102 TFEU as "What really matters is protecting an efficient competitive process and not simply protecting competitors." See Communication from the Commission 2009/C 45/02 of 24 February 2009 Guidance on the Commission's enforcement priorities in applying Article 82 of the EC (2009) OJ C 45/7 6; Case 85/76 *Hoffman-La Roche & Co. AG v Commission of the European Communities* (1979) ECR 1979-00461, para 6; Case C-52/07 *Kanal 5 Ltd and TV 4 AB v Föreningen Svenska Tonsättares Internationella Musikbyrå (STIM) upa.* (2008), para 25.
[15] Steven Anderman, 'The IP and Competition Interface: New Developments' in Steven Anderman and Ariel Ezrachi (eds), *Intellectual Property and Competition Law – New Frontiers* (OUP 2011) 5.
[16] Richard Whish and David Bailey, *Competition Law* (OUP 2018) 20.
[17] Maher Dabbah, *International and Comparative Competition Law* (Cambridge University Press 2010) 164; Alison Jones and Brenda Sufrin, *EU Competition Law: Text, Cases & Materials* (OUP 2016) 34; Whish and Bailey (n 16) 18-24.
[18] David Gerber, *Law and Competition in Twentieth Century Europe: Protecting Prometheus* (Clarendon Press 1998) 240.

than likely to say that an ordoliberal thought had a significant influence on the development of EU competition law, particularly in shaping its economic foundations. Since this phenomenon had already faced German cartels in the 1930s concerning the abuse of their economic powers, it proactively foresees a controllable economic system (instead of the Anglo-Saxon economy) to improve democracy.[19] Therefore, this conception regards some legal arrangements as necessary even though it adheres to taking a 'hands-off approach' regarding market interventions (no intervention unless it is really necessary). Although this thought was criticised by Keynesian theories several times, it was put into practice by cause celebres cases of *Consten/Grundig*[20] and *Continental Can*[21] regarding the integration of the common market.

After the Maastricht and subsequent treaties, since the beginning of the 90s, the EU has lacked enough uniformed regulations with regard to the organisation of the internal market as they commenced to proceed step by step to the common market objective. In this connection, the White Paper in 1999 gave clear signals of a new move by demonstrating that current measures were not sufficient to meet the new challenges and therefore, a more efficient system was required.[22] This process thereafter ended with the Council Regulation No 1/2003, which assured an undistorted common market with the effective and uniformed application Articles 101 and 102 of TFEU.[23] Dabbah, Jones and Sufrin named this era from 1957 to 2004 as pre-modernisation, and they claimed since that time, competition law has been in its modernisation period by adopting a consumer welfare standard based on the 'more economic approach'.[24] The accepted opinion of the economic approach has been addressed in many cases like *Intel* and *Microsoft* where a review was requested of these cases due to insufficient economic approaches and analyses. For example, the CJEU returned the *Intel* case through a lack of showing actual and likely effects (the effect-based approach) supplied with a convincing theory of harm (logically consistent counter-factual analysis supported by empirical shreds of evidence).[25]

[19] Elias Deutscher and Stavros Makris, 'Exploring the Ordoliberal Paradigm: The Competition-Democracy Nexus' (2017) 11(2) *The Competition Law Review* 181; Conor Talbot, 'Ordoliberalism and Balancing Competition Goals in the Development of the European Union' (2016) 61(2) The Antitrust Bulletin 264; Ignacio Anchustegui, 'Competition Law through an Ordoliberal Lens' (2015) 2 Oslo Law Review 139; Jones and Sufrin (n 17) 27-28.

[20] Joined Cases 56 and 58-64 *Établissements Consten S.à.R.L. and Grundig-Verkaufs-GmbH v Commission of the European Economic Community* (1966).

[21] Case 6/72 *Continental Can Company Inc. v Commission of the European Communities* (1973).

[22] Communication from the Commission 2020/C 99 I/01 of 26 March 2020 Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation) (2020) OJ CI 99/1, art 10.

[23] Council Regulation No 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002] OJ L 1.

[24] Maher Dabbah, *International and Comparative Competition Law – New Frontiers* (CUP 2010) 177-179; Jones and Sufrin (n 17) 46-49; Heike Schweitzer and Klaus Patel, 'EU Competition Law in Historical Context: Continuity and Change' in Klaus Patel and Heike Schweitzer (eds), *The Historical Foundations of EU Competition Law* (OUP 2013).

[25] Hans Zenger and Mike Walker, 'Theories of Harm in European Competition Law: A Progress Report' in Jacques Bourgeois and Denis Waelbroeck (eds), *Ten Years of Effects-based Approach in EU Competition Law* (Bruylant 2012).

Nevertheless, competition law has a dynamic structure that enables the review of actual needs and trends.[26] For instance, the Treaty of Lisbon presented different discourses such as the social market economy and securing the social justice in 2007, which are likely to change the mainstays of 'multi-purpose' objectives by considering mounting concerns such as the protection of the environment and the progression of innovation.[27] When current initiatives and jurisdictions are examined, it can be observed that competition law targets different viewpoints such as consumer protection and dispersal of economic power (welfare distribution).[28] Indeed, Vestager expansively outlined the aim of competition policy, which contributes "to efficient use of society's scarce resources, technological development and innovation, a better choice of products and services, lower prices, higher quality and greater productivity in the economy as a whole."[29] This verifies that the EC currently follows the multi-purpose objectives through considering the progression of innovation and the economy as well as other identified matters.

1.1 Innovation and EU competition law

Regarding the innovation perspective of competition law, the EC started to formulate a policy regarding science and technology at the end of the 1960s.[30] The Commission, up to present, has been of the opinion that competition law enforcement is not only beneficial to price and quality but also to the innovation process.[31] Therefore, so far, the progress and promotion of innovation have been seen as natural consequences of the protection of EU competition law rather than the phenomenon required to be protected in itself. Therefore, competition law is considered as a tool for clearing the way for innovations.[32] However, in recent years, key aspects of EU competition law underwent a

[26] For example, the EC has recently adopted a Temporary Framework, which encourages Member States to apply the 'full flexibility' for State aid rules to reinvigorate the economy during the COVID-19 pandemic. It has also published emergency guidance respecting foreign direct investments (FDI) published in March 2020 for the application of FDI Screening Regulation due to the emergent needs. See, Communication from the Commission, Temporary Framework for State aid measures to support the economy in the current COVID-19 outbreak (2020) C(2020) 1863 final; European Commission, 'State aid: Commission adopts Temporary Framework to enable member states further to support the economy in the COVID-19 outbreak' (Press Release, 19 March 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_496> accessed 14 March 2023; see for foreign direct investment updates in the period of COVID-19 outbreak, Communication from the Commission, 'Guidance to the Member States concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of Regulation (EU) 2019/452 (FDI Screening Regulation) (2020) C(2020) 1981 final.

[27] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C 306, art 3.

[28] Whish and Bailey (n 16) 18-24; Jones and Sufrin (n 17) 28-34.

[29] European Commission, 'EU competition policy in action' (2016) 9 <https://ec.europa.eu/competition/publications/kd0216250enn.pdf> accessed 14 March 2023.

[30] Schweitzer and Patel (n 24).

[31] Pablo Ibáñez Colomo, 'Restrictions on Innovation in EU Competition Law' (2016) 41(2) European Law Review 202.

[32] Pieter Cleynenbreugel, 'Innovation in competition law analysis: making sense of on-going academic and policy debates' in Paul Nihoul and Pieter Cleynenbreugel (eds), *The Roles of Innovation in Competition Law Analysis* (Edward Elgar 2018).

radical change that IP-based considerations superseded to price-output considerations as can be seen in cases of *Motorola*[33] and *Lundbeck*.[34]

However, the extent to which EU competition law overcomes problems about innovation as the Commission has not determined any benchmarks to elucidate future competition law analysis. This is because the place of innovation can be questioned in EU competition law is a vague moot point among scholars whether and to what extent it exists within the structure of the theory of harm.[35] Ibáñez Colomo argues there are static concerns of EU competition law because this kind of approach based on static variables can only provide a solution for short terms, this is to say, likely affects the technological progress (rather than creating or cementing market power) can only be discovered as long as a dynamic understanding is developed.[36] Kerber also considers forming innovation-emphasised assessment concepts instead of traditional concepts obligatory in compliance with the digital revolution wave, which has a potential to change the whole legal thinking by virtue of the fact that all new concepts of digitalisation such as big data, artificial intelligence (AI), and algorithms likely pose problems in terms of markets.[37] In this regard, it is important to mention that the EC and European courts are currently experiencing difficulties with making relevant market definitions. Akman,[38] Robertson,[39] Ferro[40] and several other scholars[41] state that EU competition law should redress itself by generating analytical tools for establishing harm theories in relation to digital markets and other forthcoming innovative markets.

Creating market definitions is a legal obligation in EU competition law assessments, as indicated by the court in its Continental Can decision, which determined that the EC must define the market and show that a dominance position was held to reach a decision.[42] The initial phase of a "market power" judgment is the determination of the relevant market and whether the use of market power in this market has anti-competitive outcomes. In this regard, market power was defined in the United Brands and Hoffmann-La Roche cases

[33] Case *Motorola – Enforcement of GPRS Standard Essential Patents* (2014) C(2014) 2892 final.
[34] Case *Lundbeck* (2013) C(2013) 3803 final.
[35] Cleynenbreugel (n 32) 2.
[36] Ibáñez Colomo (n 31) 202-203.
[37] Wolfang Kerber, 'Competition, Innovation, and Competition Law: Dissecting the Interplay' (Joint Discussion Paper Series in Economics No 42-2017, 2017) 1 <https://www.semanticscholar.org/paper/Competition%2C-Innovation%2C-and-Competition-Law%3A-the-Kerber/5c779025e7163b9726ef9d110d4da32bc8c350e1> accessed 14 March 2023.
[38] Pınar Akman, 'Competition Policy in a Globalized, Digitalized Economy' White Paper, World Economic Forum (December 2019) <http://www3.weforum.org/docs/WEF_Competition_Policy_in_a_Globalized_Digitalized_Economy_Report.pdf> accessed 14 March 2023.
[39] Viktoria Robertson, 'Antitrust Law and Digital Markets: A Guide to the European Competition Law Experience in the Digital Economy', in Heinz D. Kurz and others (eds), *The Routledge Handbook of Smart Technologies: An Economic and Social Perspective* (Routledge 2020).
[40] Miguel Ferro, *Market Definition in EU Competition Law* (Edward Elgar 2019).
[41] Ariel Ezrachi and Viktoria Robertson, 'Competition, Market Power and Third Party Tracking' (2019) 42 World Competition 5; Bruno Deffains, Olivier d'Ormesson and Thomas Perroud, 'Competition Policy and Industrial Policy: for a reform of European Law' (2020) <https://www.robert-schuman.eu/en/doc/divers/FRS_For_a_reform_of_the_European_Competition_law-RB.pdf> accessed 14 March 2023.
[42] *Continental Can* (n 21) para 32.

as "a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately of its consumers."[43] Although a broad market definition has been made, more than 40 years have passed since these decisions. During this period, the evaluation of new economic developments and changing market structures (such as multisided platforms, zero-price and data-centric digital markets) have been left entirely to the EC's margin of appreciation through defining and assessing the relevant market. The EC accordingly makes detailed market analyses as such in the *Google Shopping*[44] and *Google Android*[45] cases in accordance with the more economic approach. However, arguably, there is a lack of examining pre-market conditions and competition in innovation in R&D markets, where businesses are competing to make more innovative products. While defining the relevant market and market power, the things to look at in today's technology-intensive markets should also be granted patents and the capacity to innovate, apart from traditional criteria such as determining the market share in a specific geographic market. Hence, the EC should emphasis on making market analyses by specifically assessing R&D markets within its margin of appreciation to establish more comprehensive and fitted determinations. This kind of approach will likely enable to react with dynamic reflections against dynamically expanding business models and market structures.

Dynamic competition is a fundamental characteristic of the new economy. This causes a breakthrough change in the elements of competition as competition in the level of innovation substitutes the competition in price. In other words, while traditional markets consist of static competition where businesses capitalise on the comparative cost advantage, latter-day markets have a dynamic character as businesses are competing based on their innovations. Porter, accordingly, expressed that modern competition hinges upon productivity rather than having access to resources. This productivity is a form of innovation, which is one of the most effective tools to bestow competitive capacity.[46] This actuality promotes and even necessitates making a considerable R&D investment. The terms 'promote' and 'necessitate' are intentionally distinguished. The new economy encourages businesses to make innovation because they can gain favour from the network externalities, the first-move advantage and the low marginal cost even if there is a risk of facing enormous sunk costs.[47] It also necessitates businesses to adapt to such innovation-making strategies to make their presence felt, or otherwise, they will presumably have no more market power.

[43] Case 27/76 *United Brands Company and United Brands Continental BV v Commission* (1978) ECR 207, para 65, and *Hoffmann-La Roche* (n 14) para 38.
[44] *Google Search (Shopping)* (2017) C(2017) 4444 final.
[45] Commission Decision C(2018) 4761 final of 18 July 2018 relating to a proceeding under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.40099 – Google Android).
[46] Michael Porter, 'Clusters and the New Economics of Competition' (1998) 76(6) Harvard Business Review 77.
[47] OECD, 'The New Economy Beyond the Hype: Final Report on the OECD Growth Project' (Meeting of the OECD Council at Ministerial Level, 2001) 41-86 <http://www.oecd.org/economy/growth/2380634.pdf> accessed 14 March 2023.

Overall, this dynamic structure of the new economy assures the prevention of monopolisation of businesses unless they provide innovation. In contrast, if continuous innovations are provided, monopolisation arguably becomes harmless.[48] Despite the fact that the new economy seems to be able to self-regulate itself in theory, the main argument of the state interventionists is based on the view that monopolistic formations will likely eliminate the courage of other firms to innovate.

As a consequence of that, states ought to remove the likely obstacles of innovative process in order to maximise consumer welfare as well as to protect other businesses. On the contrary case, monopoly businesses may impose on their rivals to use their operative systems or to make tied selling.[49] These examples, of which more exist, present danger of the suppression of innovation. To the extent that the progression of innovation is disrupted, both consumer welfare and the innovation-driven economy are affected negatively. Therefore, it appears that all conduct, which is prejudicial to the development of innovation, ought to be dogmatised as unlawful, notwithstanding any other dynamics in the new economy. It is quite apparent that there is a need for more innovation-focused policies and analyses. Studies also affirmed that developing a consistent policy is a must for the promotion of innovation inasmuch as uncertainties in policies negatively affect the quality and quantity of innovation.[50]

It seems that in the orientation period of dynamic efficiency in competition law enforcement, it would likely be to examine to what extent businesses contribute to innovation before arriving at a penalty conclusion regarding competition law infringements. However, one may raise the question the extent to which such efficiency defence is regarded as juridically acceptable (even though it is not easy to apply it in practice) because a similar efficiency defence was accepted in *Intel* whereas it was rejected in *Magill*. Therefore, there is no obstacle to put forth an 'innovation defence' as an additional objective justification considering Article 102 TFEU. In another saying, defendants can basically assert an innovation defence while plaintiffs are entitled to stay loyal to structuralist arguments. In the face of such a situation, although EU competition authorities have preferred structural dominance analyses (such as cost-benefit analysis) pursuant to narrow market interpretation, nevertheless it is required to make a point of considering cogent grounds of defendants.[51] In spite of the difficulty to measure non-economic efficiencies such as innovative and environmental benefits, taking a futuristic approach seems necessary.[52] However, at the same time, she has been criticised in relation to the stifling of innovation due to massive fines levied by the Commission against

[48] Giorgio Monti, 'EC and New Economy Markets' in Cosmo Graham and Fiona Smith (eds), *Competition, Regulation and the New Economy* (Hart 2004).
[49] Robert Hahn, 'A Primer on Competition Policy and the New Economy' (2001) 1 Milken Institute Review 38.
[50] Utpal Bhattacharya and others, 'What Affects Innovation More: Policy or Policy Uncertainty?' (2017) 52(5) Journal of Financial and Quantitative Analysis 1869.
[51] Monti (n 48) 49.
[52] This kind of approach is supposed to be adapted to protect other public interests such as innovation and the environment alongside the price and quality of products.

technology companies such as Google and Qualcomm.[53] It is quite evident that the progression of competition and innovation ought to be taken into consideration together rather than expecting more innovation ipso facto by only protecting competition.

1.2 Actual and potential problems concerning the impediment of innovation in terms of EU competition law

Recently, the EC's general attitude in its competition analyses has shifted towards an IP-based approach, especially in the high-tech industries. This means that competition analyses (and enforcements) no longer confine with only price-quality considerations but also innovation considerations.[54] However, it remains uncertain how the Commission handles innovation- related problems since it has not determined any criteria in reference to its analyses. This uncertainty arises from the static standpoint of the Commission while specifying the impact of innovation is required to have a more dynamic standpoint, because long-term outcomes of innovation considerations are too complex to show their likely effects on the technological process, the market, and the consumer welfare. Ibáñez Colomo attributed this challenge to 'quintessentially static in nature' structure of EU competition law.[55]

Ibáñez Colomo, accordingly, argues that innovation has only an indirect effect on EU competition law analysis according to contemporary decisions of the CJEU.[56] When these decisions are examined by only taking account of Article 102 TFEU-related cases, it can be said that there are some certain practices, which are deemed per se anti-competitive regardless of their influences on the competitive structure such as exclusive dealing and loyalty rebates.[57] In respect to some other practices, it is necessary to show anti-competitive effects by instantiating as it is the case with margin squeeze practices and selective price cuts.[58] However, it would not be sufficient to show the influences of these practices on between price and output because the CJEU does not only prohibit practices that directly harms to consumers but also the competitive process. In this regard, it has to be primarily addressed the *TeliaSonera* case in which it was determined that "… an undertaking which holds a dominant position has a special responsibility not to allow its conduct to impair genuine undistorted competition in the internal market."[59] That means

[53] Geoffrey Manne, 'The EU's Google Android antitrust decision falls prey to the nirvana fallacy' (Truth on the Market, 18 July 2018) <https://truthonthemarket.com/2018/07/18/the-eus-google-android-antitrust-decision-falls-prey-to-the-nirvana-fallacy> accessed 14 March 2023; Dirk Auer and others, 'Why the Commission's Google Android decision harms competition and stifles innovation' (Truth on the Market, 18 July 2018) <https://truthonthemarket.com/2018/07/18/why-the-commissions-google-android-decision-harms-competition-and-stifles-innovation> accessed 14 March 2023.
[54] Ibáñez Colomo (n 31) 202.
[55] ibid 203.
[56] ibid.
[57] *Hoffmann-La Roche* (n 14) para 89.
[58] C-209/10 *Post Danmark A/S v Konkurrenceradet* (2012), paras 34-39.
[59] Case C-52/09 *Konkurrensverket v TeliaSonera Sverige* (2011), para 24.

Article 102 TFEU does not only deal with practices causing direct harm to consumers but also other practices causing harm to consumers because of their impacts on competition.[60] It is possible to interpret this development as referring that there are other parameters, which can harm to consumers indirectly rather than price and output.

Thus far, EU competition law has inspirited the progress of innovation to an extent as it paid to regard the increase of competition, which spurs innovation, by considering quality/price trade-off. However, considering the current discussions, it seems that innovation becomes a part of this classical trade-off discourse. That is to say, innovation is shown as such a 'skeleton key' to resolve the problems from economic growth to climate change.[61] On top of that, as EU competition law professes to regulate innovation, it ought to focus its attention on evaluating and addressing 'harm to innovation' through considering assets granting innovation capabilities. It also should be obliged to throw light on a comprehensive analysis, including innovative capacity with respect to examine market power.[62]

For instance, existing (traditional) competition law tests seem insufficient to measure potential harms as it has been mostly ignored the impact of innovation and economic benefits of foreclosed innovation.[63] Therefore, one may argue that the EC ought to concentrate on investigating a network (rather than a simple market analysis), the rate of innovation by benefiting from its historical roots (rather than focusing on price/quality trade-off) and barriers to make innovation (rather than barriers to market entry).[64] However, Monti argued against this transformation and found it speculative because of two reasons: (1) the hardship to transfer these phenomena into practice, (2) these suggestions are inimical to EU competition law culture as it stands now.[65] Indeed, assessing competition over innovation is a sticky situation with a static point of view. However, it is far from impossible to incorporate innovation considerations into competition law analyses and enforcements.[66] For example, the introduction of new products, the

[60] Case 322/81 *Nederlandsche Banden-Industrie-Michelin v Commission* (1983) ECR 3461, para 57; Joined Cases C-395/96 P and C-396/96 P *Compagnie maritime belge transports and Others v Commission* (2000) ECR I-1365, para 37; Case C-202/07 P *France Télécom v Commission* (2009) ECR I-2369, para 105.

[61] European Commission, Expert Group on Evaluation Methodologies for the Interim and Ex-post Evaluations of Horizon 2020, 'Applying relevance-assessing methodologies to Horizon 2020' (February 2017).

[62] Francisco Costa-Cabral, 'Innovation in EU Competition Law: The Resource-Based View and Disruption' (2018) 37 Yearbook of European Law 305.

[63] Kevin Caves and Hal Singer, 'When the Econometrician Shrugged: Identifying and Plugging Gaps in the Consumer Welfare Standard' (2018) 26(2) George Mason Law Review 1.

[64] Note, 'Antitrust and the Information Age: Section 2 Monopolization Analyses in the New Economy' (2001) 114 Harvard Law Review 1623.

[65] Monti (n 48) 35-36.

[66] In merger control, the EC gave the first signals of this move in *Deutsche Börse* by making clear references to innovation considerations. According to this case, the Commission determined that the proposed merger between Deutsche Börse AG and NYSE Euronext Inc. has a potential to very likely increase exchange fees and decrease innovation because of the decrease in offered platforms to consumers. As stated by the Commission, the disappearance of intensive competition in innovation would likely be a foregone conclusion as well as a 'non-negligible' incentive decrease to innovate. This is because concentration parties trigger each other, and they would not have any drivers to innovate in terms of product

frequency of launching those products or the improvements (upgrades) of existing products may provide an insight into competition dynamics.

Innovation-related claims have no place to assert in competition law analysis because of the difficulty of verifying innovation-related efficiency claims, which are ambiguous outcomes in the long run. Taking this issue a step further, one may argue that innovation by its very nature and elusiveness is not conducive to be a subject of such analysis. From another angle, it is also next to impossible to show the causal link between relevant practice and the process of innovation.[67] For example, Microsoft raised suchlike claim that restraints on its IP rights by being compelled to offer interoperability for its products annihilate incentives to make innovation because its profit expectation in return to reserved budget for research and development investments is interrupted. However, not surprisingly, the General Court affirmed the Commission's analyses, which found Microsoft's claims inadequate, vague, general and theoretical because Microsoft fell short of specifying which technologies in what way are affected. This is because Microsoft simply stated that "disclosure would ... eliminate future incentives to invest in the creation of more intellectual property" without specifying the technologies or products to which it thus referred.[68] However, it can be said that the Commission left the door open to make further claims through better and provable arguments as much as it sounds difficult.

2 The increase in innovation-related considerations by the EC

The consideration of innovation appears more in most recent EU competition law cases in comparison with the decisions has taken during the 20th century. Hence, this consideration can be regarded as a new trend. It is irrefutable that the Commission uses its reasonable efforts to boost innovation against all the odds mentioned so far. For instance, it stipulates that dominant businesses have to cooperate with other undertakings in light of FRAND (fair, reasonable and non-discriminatory) conditions as it was the case with *IMS Health*[69] and *Aéroports de Paris*.[70] Therefore, exclusionary practices of dominant businesses have been regarded as unlawful to encourage innovation by furnishing an occasion to other firms to benefit from the network of dominant businesses through linking

innovation if the merger was accepted. At this point, the EC was not convinced to change its consideration coming from its preliminary conclusion, as parties did not put forward to any valid evidence in the presented statement of objections even though they made some commitments regarding the continuity of innovation to some degree. It is obvious that the EC has questioned the dimensions of workability and effectiveness of claims rather than whether the presented remedies are sufficient. This manner validates the thoughts of Monti regarding the impracticability of applying innovation analysis under existing legal standards. See Case T-175/12 *Deutsche Börse AG v European Commission* (2015), para 138; Commission Decision Case No COMP/.6166 *Deutsche Börse / NYSE Euronext* (2012) C(2012) 440 final, para 635; Monti (n 48); Jones and Sufrin (n 17) 1197.

[67] Ibáñez Colomo (n 31) 201-219.

[68] Case T-201/04 *Microsoft Corp* (2007), para 698.

[69] Case C-418/01, *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG* (2004).

[70] Case C-82/01 *Aéroports de Paris v Commission of the European Communities* (2002).

their goods and services to this network.[71] In contrast, it can also be seen that EU case law does not presume practices directly abusive (unlawful) in terms of Article 102 TFEU just because they leave competitors in a difficult situation. Before intervening in such practices, the Commission wants to see whether they exceed predetermined thresholds, where actual and potential exclusionary effects of those practices on rivals are brought to light with a minute inquiry.[72] For instance, the Commission determined that refusal to license practices would not be evaluated as an abuse of market dominance in general if this license is not indispensable and therefore, it does not affect downstream market competition.[73] Likewise, it was determined in *Post Danmark I* that selective price cuts would not constitute an abuse of dominance unless the relevant undertaking excludes its competitors and limits their ability (and incentives) to innovate in the long run.[74] In reference to more recent cases, the Commission fined Google to €2.42 billion because of abusing dominance for the reason that Google does not level the playing field in terms of every competitor in its shopping search service, which provides price comparison of selected businesses. To put it in a different way, this service prevents European consumers from taking full advantage of potential innovation because other rivals have not enough incentive to innovate as they do not have the same opportunity. One of the significant preliminary conclusions of the Commission concerning Google is below:

> Google's conduct has a negative impact on consumers and innovation. It means that users do not necessarily see the most relevant comparison-shopping results in response to their queries, and that incentives to innovate from rivals are lowered as they know that however good their product, they will not benefit from the same prominence as Google's product.[75]

It can be stated that innovation considerations were taken into consideration in the first phase. However, the general approach of the Commission remains to be seen because it is hard to take to any means from this statement. On the one hand, a more likely scenario, this innovation consideration stems from an apprehension of excluding rivals. On the other hand, one may put forward that the essence of the matter restricts the competition. On top of that, the point to consider from the statement is to specify an innovation consideration irrespective of the connotation under which meaning as the word of innovation is not frequently used. Article 102 TFEU and innovation have been strongly linked in Google Search (shopping) as stated in the following:

[71] Monti (n 48) 48.
[72] Ibáñez Colomo (n 31) 201-219.
[73] C-241/91 P and C-242/91 P *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP)* (1995); *IMS Health* (n 69). See also, Case C-280/08 *P Deutsche Telekom AG v European Commission* (2010) I-09555, paras 70-71.
[74] *Post Danmark A/S v Konkurrenceradet* (n 58), para 38.
[75] European Commission, 'Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android' (Fact Sheet, Brussels, 15 April 2015) <https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4780> accessed 14 March 2023.

> […] [T]he Conduct is likely to reduce the incentives of competing comparison-shopping services to innovate. Competing comparison shopping services will have an incentive to invest in developing innovative services, improving the relevance of their existing services and creating new types of services, only if they can reasonably expect that their services will be able to attract a sufficient volume of user traffic to compete with Google's comparison-shopping service. Moreover, even if competing comparison shopping services may try to compensate to some extent the decrease in traffic by relying more on paid sources of traffic, this will also reduce the revenue available to invest in developing innovative services, improving the relevance of their existing services, and creating new types of services.[76]

The Commission enunciated that Google's shopping service has a potential to undermine the competitive process because it leads to a stalemate their rivals and consumers as these practices will result in higher fees for merchandisers, higher costs for consumers and fewer innovation incentives.[77] The probable and proximate cause of using the expression of less innovation reflects the firm position of the Commission that exclusionary practices restrict innovation because of reducing the number of competitors in the market. Analyses related to innovation process (on practices regardless of the suppress or contribute to innovation) becomes a deep-seated taboo, which remains a challenge for EU competition law, and it seems like it will continue to do so. It is more than likely that the difficulty in specifying a standard of proof is one of the main reasons of this challenge because it is always questionable which practices are detrimental to the innovation process. On the other hand, it also goes without saying that a practice enhances innovation will not be directly regarded as a pro-competitive action.[78]

2.1 The current perspective of the EC on innovation

Regarding the EC's competition analyses, the progress of innovation is considered part of the assessment to establish a harm theory in merger cases,[79] whereas it is not investigated in cases related to Article 102 TFEU. However, there are some innovative considerations between the lines of antitrust-related cases. The EC's approach to innovation is examined below by determining its position in both antitrust and merger cases.

[76] *Google Search (Shopping)* (n 44), para 595.
[77] ibid para 593.
[78] Although all considerations are apt to utter impracticability of incorporating innovation process (capability), the issue was reframed in the Dow/DuPont merger procedure. However, it should be noted that the Commission's approach to antitrust and merger cases are different.
[79] Vincenzo Denicolò and Michele Polo, 'The Innovation Theory of Harm: An Appraisal' Bocconi Working Paper N. 103 (March 2018) <https://repec.unibocconi.it/iefe/bcu/papers/iefewp103.pdf> accessed 14 March 2023.

2.2 The EC's approach to innovation in Antitrust matters

The current understanding of EU competition law covers several competitive parameters that affect consumer decisions, such as price, quality, choice and innovation.[80] Even though the EC has developed criteria to evaluate price, quality and choice-related conflicts, it is unclear how the EC investigates innovation-related conflicts because EU competition law remains incapable of assessing dynamic features of innovation.[81] Moreover, it is not clear how innovation might be improved or to what extent national level approaches will encourage businesses to innovate. For example, the French Competition Authority has decided that Nespresso (a coffee machine and coffee pod manufacturer) must share technical information with its competitors 18 weeks before introducing a new product.[82] This determination can be interpreted as a way of liberalising innovations from Arrowian perspective, whereas it can also be regarded as disincentivisation for Nespresso making further innovations from a Schumpeterian view. Yet, there is precedent in EU competition law to observe a European approach in this regard, but no matter which approach the EC employs, its primary aim needs to balance incentives for innovation and investment.

Among innovation-related issues, there are predatory innovations that eliminate the competition while providing no consumer benefit.[83] These innovations can arise from modifications to technology uses or product technical designs, preventing technology compatibility and other existing operations provided by third parties.[84] Put simply, preventing competitor access to innovation poses an obstacle to sustainable competition.[85] Given this context, the EC found in the Microsoft case that hindering the competitiveness of its competitors was unlawful through providing essential facilities on Microsoft's own platforms. In other words, the EC prevented innovative initiatives of other companies from being suppressed.[86] Consequently, Microsoft has been found guilty of preventing users from accessing competing software (though it is worth noting that integrating its own sub-product does not constitute an anti-competitive character per se).[87]

[80] C-209/10 *Post Danmark A/S v Konkurrencerådet* (n 58), para 22; Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between data protection and competition in EU Law' (2017) 54(1) Common Market Law Review 17; Case C-413/14 P *Intel* (2017), para 134.
[81] This issue was discussed in section 3. For further discussion, see, Ibáñez Colomo (n 31).
[82] L'Autorité de la Concurrence (The French Competition Authority) 'Nespresso ruling of the French Competition Authority' [2014] n 14-D-09.
[83] Janusz Ordover and Robert Willig, 'An Economic Definition of Predation: Pricing and Product Innovation' (1981) 91(1) Yale Law Journal 8-53; Thibault Schrepel, 'Predatory Innovation: The Definite Need for Legal Recognition' (2018) 21 SMU Science and Technology Law Review 22.
[84] Janusz Ordover and Robert Willig, 'An Economic Definition of Predation: Pricing and Product Innovation' (1981) 91(1) Yale Law Journal 9.
[85] Commission Decision Case *Beh Gas* (2018) C(2018) 8806 final.
[86] Roberto Pardolesi and Andrea Renda, 'The European Commission's Case Against Microsoft: Kill Bill?' (2004) 27 World Competition and Economics Review 513.
[87] Case T-201/04 *Microsoft Corp* (2007), paras 101-336.

This approach was repeated in the Qualcomm case as follows: "Where a holder of the IP right is regarded as enjoying a dominant position, the requirement that the use of those IP rights be non-abusive cannot be regarded as insufficient reward in the light of the incentives for innovation".[88] Another example in the *Google Shopping* case indicated "the conduct decreasing traffic from Google's general results pages to competing comparison shopping services, in contrary increasing traffic from Google's general search results pages to Google's own comparison shopping service" and found this anti-competitive, as it was likely to reduce innovation incentives when competing in comparison-shopping services.[89] Furthermore, the EC mentioned the terms 'reducing innovation' and 'deterring innovation' in the *Google Android* case.[90] In light of these, it can be claimed that suppression of innovation claims are somewhat covered by EU competition law, and open to investigation under Article 102 TFEU. The EC also verified the application of that article in innovation-intensive markets (e.g., fast-growing sectors, such as software) despite these markets being characterised by short innovation cycles, and therefore, temporary dominant positions.[91]

Overall, the EC took a view of ensuring that consumers could switch their services freely in case of price escalation or innovation discontinuance,[92] considering competition and innovation to be beneficial as long as customers have an option to switch providers. Simply, the EC eliminates all anti-competitive obstacles to provide an impetus for innovating businesses. One of the most important goals of the EU is to provide an open market economy with free competition;[93] consequently an undistorted competition environment must be created to ensure free competition. Therefore, removing obstacles to the dynamic development of innovation is the most important action, ensuring all market players' ability to innovate and guaranteeing free competition. Since innovation is of great importance to the consumer and market perspectives, Article 102 TFEU should be interpreted in a broader sense.[94] However, due to the uncertain nature of innovations (because of the unpredictable and dynamic nature of innovation), it remains unclear to what extent competition law interventions would be pro-consumer.[95] In light of all these, Ezrachi has developed the term 'cautious intervention' in relation to innovation in the

[88] Commission decision Case *Qualcomm* (predation) (2019) C(2019) 5361 final, para 265; Case C-457/10P *AstraZeneca* (2012), para 273.
[89] *Google Search (Shopping)* (n 44), paras 591, 595.
[90] In the decision, it was mentioned that it is possible to lower the quality or reduce the innovation since Google has absolute control over the development of Android versions. In addition to this, it was concluded that the tying of the Google Search app with the Play Store helps Google to deter innovation because it prevents other specific mobile web browsers with innovative features. See *Google Android* (n 45), paras 573, 723, 773, 858, 896, 969, 1139.
[91] *Google Search (Shopping)* (n 44), para 267; *Qualcomm* (n 88), para 260; Case T-79/12 *Cisco Systems, Inc. and Messagenet SpA v European Commission* (2013), para 69; *Google Android* (n 45).
[92] Cisco Systems, Inc (n 91), para 52.
[93] See Articles 119, 120, 127, 170 and 173 TFEU.
[94] C-209/10 *Post Danmark A/S v Konkurrencerådet* (n 58) para 22.
[95] Josef Drexl, 'Anti-competitive stumbling stones on the way to a cleaner world: protecting competition in innovation without a market' (2012) 8(3) Journal of Competition Law and Economics 507; Schrepel (n 83) 19.

context of EU competition law.[96] That being said, it is observed in the current situation that detailed analyses on innovation have not been carried out and that concerns about innovation development remain between the lines without influencing judgements. Nevertheless, it is possible to indicate henceforward that innovation can be examined as an independent parameter of competition law. With this understanding, enforcement against the suppression of innovation would be a concomitant result.

2.3 Innovation considerations in merger analyses

From a broad perspective, identifying the EC's standpoint on innovation by examining the case of *Dow/DuPont* in relation to merger control would be beneficial. However, it should be noted that merger and antitrust analyses have completely different characteristics. The agreed upon merger of *Dow/DuPont*[97] successfully epitomised the role of innovation in merger analyses. The EC assessed the innovative strengths of Dow and DuPont by analysing all patents granted them from 2000 to 2015.[98] The investigation was launched under the concession that competition in the pesticide production market is based on innovation. Hence, the existence of innovation competition was accepted in advance as the competition reflected a dynamic patent race between five companies (previously known as big 5), namely BASF, Bayer, Syngenta, Dow and DuPont. It has been observed that farmers are inclined to purchase new products, including those that are less toxic but contend effectively with various types of pests. Therefore, the decrease in innovation is an undesired result since the rate of the competition will concordantly diminish. The main concern regarding the given merger was the likelihood of decreasing innovation since Dow and DuPont triggered each other to innovate while they were competing head-to-head. Other concerns were the decrease in the number of market players and the high market entry barriers to having similar research and development capacity if this merger would have happened.[99] According to the conditional acceptance of this merger, it has been found appropriate to transfer (alienate) the large part of pesticide business and related research and development organisations. In this premise, it was agreed that the merger would not make any changes regarding the incentives to

[96] Ariel Ezrachi, 'The Goals of EU Competition Law and the Digital Economy' (Oxford Legal Studies Research Paper No. 17/2018, 2018) 2-22 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191766> accessed 14 March 2023.
[97] Commission Decision of 27.3.2017 declaring a concentration to be compatible with the internal market and the EEA Agreement (Case M.7932 – *Dow/DuPont*) (2017) C(2017) 1946 final.
[98] ibid para 2447.
[99] ibid paras 222, 453, 498, 1955-3297.

pursue parallel innovation efforts.[100] In brief, the EC considered restrictions in the level of R&D capabilities in the given circumstances.[101]

Dow/DuPont merger investigation riveted innovation on to other parameters of competition law, namely price, choice, and quality. Such a transition from traditional sources of competition law to more dynamic and contemporary parameters incisively fulfil the changing needs when considered that markets are not solely determined by static power anymore, but by disruptive innovations having dynamic characteristics. Therefore, innovation can be suitably accepted as a counterbalance to market power. Even if a detailed analysis of the Dow/DuPont merger was presented through showing likely effects on innovation competition, there was a lack of due diligence to show the causal link between the merger and further innovation activities. The EC had a reasonably abstract approach to conclude without establishing how future product innovations are restricted and without establishing a specific link to existing or future markets.[102] The theory of harm in the Dow/DuPont can be based on the mostly referred concerns mentioned throughout the analysis, such as discontinuation, delay or redirection of research activities. One may argue that these concerns represent forward-looking apprehensions, which may enlighten the subsequent decisions, which will likely embody with future innovation (market) estimations. It would not be wrong to say that this decision is a milestone in terms of showing the importance given to innovation considerations. However, an endeavour to examine innovation seems quite insuperable as it is not conducive to be a subject of any standard of proof because of its vagueness (forecast uncertainty). Indeed, the very likely reason why the EC did not differentiate between research and development activities and innovation was to go through the hardship of formulating innovation. This is because, for example, overspending budget for R&D activities does not mean to achieve more innovation even if it supports to innovate.

It appears from the said investigations that several attempts have been conducted to find out the effects of the innovation process in competition law analysis. Even though the Dow/DuPont decision brought a novel dimension to the application of innovation in merger control analysis by considering research and development capabilities of merged parties, the dispute still continues with regard to innovation considerations in EU competition law.[103] The transition towards innovation considerations has already begun by Deutsche Börse, but Dow/DuPont gave supporting signs to proceed with more

[100] European Commission, 'Mergers: Commission clears merger between Dow and DuPont, subject to conditions' (Press Release, Brussels, 27 March 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_772> accessed 14 March 2023.

[101] Bundeskartellamt, 'Innovations – Challenges for competition law practice' (Series of papers on "Competition and Consumer Protection in the Digital Economy" November 2017) 2 <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Schriftenreihe_Digitales_II.pdf?__blob=publicationFile&v=3> accessed 14 March 2023.

[102] ibid 30.

[103] It should be noted that competition law (antitrust) and merger control depend on different analysis in terms of ex post and ex ante analysis. However, it is important to be aware of non-Article 102 TFEU considerations like merger control because the mindset behind decisions serve at same purposes.

innovation-focused analyses.[104] In furtherance to this, an investigation has just been initiated against BMW, Daimler and Volkswagen on the grounds that they debarred European consumers from existing emission cleaning technologies from 2006 to 2014 in light of Article 101/1(b) TFEU (whether there is a likely cartel agreement to limit or control production, markets or technical developments). These German car manufacturers are now under investigation to not to prevent environmental damage even though they have preventive technology as stated in the preliminary view of the Commission.[105] Therefore, this investigation fundamentally attests that the Commission examines thoroughly different dimensions such as existing underutilising technologies (a type of suppression of innovation) and considering environmental perspectives alongside with price, quality, and choice trilogy. All these recent happenings show that EU competition law employs more comprehensive approach in merger analyses by paying strict attention to the progression of innovation through removing all the impediments, which may harm to innovation, in both investigation and proceeding phases.

3 Theoretical analysis of impeding innovation in terms of competition and intellectual property laws

The aims of competition and IP laws are prima facie considered as intertwined because IP law bestows monopoly rights to inventors, which can result in more monopolised market structure. However, these laws complement each other, and they are both instrumental to promote innovation.[106] Therefore, they are required to be addressed regarding innovation suppression practices. For several reasons, some innovations are presented late or, even worse, not presented at all, which may imply the suppression of innovation, though not always. This scenario arises from patent holders' practices, in which they use their monopoly powers originating from their IP rights to halt the progress of innovation. The US antitrust law literature took an interest in the innovation suppression concept (it is also called technology suppression) to some extent, whereas EU competition law has not placed any focus on this concept so far. In this regard, this chapter strives to carry this significant discussion across the ocean as members of the EU are faced with the same difficulties in different names.

The suppression of innovation becomes apparent in different forms, but cases hinge upon patent rights since these rights lend themselves to abuse (misusing or no using) of the introduction of new technologies. Patent rights, standing alone, are lawful in the

[104] Ibáñez Colomo (n 31) 561-2.
[105] European Commission, 'Antitrust: Commission sends Statement of Objections to BMW, Daimler and VW for restricting competition on emission cleaning technology' (Press Release, Brussels, 5 April 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2008> accessed 14 March 2023.
[106] Gustavo Ghidini, *Intellectual Property and Competition Law: The Innovation Nexus* (Edward Elgar 2006) 99; Jonathan Turner, *Intellectual Property and EU Competition Law* (OUP 2010) 3; David Encaoua and Abraham Hollander, 'Competition Policy and Innovation' (2002) 18 Oxford Review of Economic Policy 63.

normative sense. However, legal assessment becomes complicated when patent holders conduce towards suppression of innovation, as in the case of non-use of patents, as there is no actual violation of competition law in the normative doctrine. Therefore, there is a need to designate a legal standard proof to prevent such suppression activities via competition law tools. Nevertheless, this kind of standard can be bending easily. For instance, an undertaking may be found to suppress technology if it does not sufficiently concentrate on research activities. Although these example scenarios have merit to an extent, it is challenging to lay the groundwork for making such provisions. Even though the practices cause technology suppression, it does not mean that they are anti-competitive. Hence, evaluation on a case-by-case basis is required to separate anti-competitive and unlawful conduct. Throughout this chapter and the following chapters, specific technology suppression cases will be argued.

3.1 Impeding innovation as an anti-competitive practice

The concept of innovation suppression was leastwise put into word in the US Antitrust law, whereas it is a genuinely new concept for the EU competition law.[107] The question that should be asked about the suppression of innovation is whether there is a real competition law violation by determining what purpose of the law is impinged in this framework. According to Peritz, competition law is a composition of regulating private economic activities for the sake of the development of the public interest.[108] As to EU competition law, it aims to provide consumer welfare, which is an ever-expanding concept in following the acceptance that consumer welfare covers the low price, high quality, and wider choices. However, as this study claims, current concerns like promoting innovation ought to be addressed in competition violation assessments because businesses are now getting competitive power upon their innovativeness. Therefore, it is necessary to take preventive measures to secure the progress and promotion of innovation in the context of EU competition law, against innovation suppression practices.

To set a framework for this concept, it would be beneficial to address Flynn's quadripartite analysis that evaluates the extent to which preventing, deterring or suppressing innovation are contrary to the EU competition law in light of considering private interests in addition to the public interest.[109] The market regulator, accordingly, ought to ensure the dispersion of supremacy, the elevation of merit competition, the pleasure of consumers and the protection of the competitive process. Therefore, the competition policy needs to ensure three basic forms of economic efficiency, namely

[107] Note that this concept is much more called as technology suppression in US Antitrust law rather than innovation suppression.
[108] Rudolph Peritz, 'A Counter-History of Antitrust Law' (1990) 39(2) Duke Law Journal 263.
[109] John Flynn, 'Antitrust Policy, Innovation Efficiencies, and the Suppression of Technology' (1998) 66 Antitrust Law 492.

allocative, productive and innovation efficiencies.[110] In other words, the policymaker should secure the continuity of innovations and the dispersion of these innovations to consumers and rival corporate entities without interruption. Nevertheless, when it comes to practice, it is not easy to assess these efficiencies as they mostly rest upon estimations. Hence, it is evident that practical difficulties will be occurred with regard to make a counter-factual analysis and to show an actual effect and proof of purpose.[111] In parallel, the question of 'what would have occurred but for suppressing technology instead' can be rested upon factual reasons, this question will likely remain puzzled.

Even though there is no merit to discuss which efficiency is superior to others, Brodley is of the opinion that innovation efficiency is the most important one to 'provide the greatest enhancement of social wealth'.[112] However, the difficulty to prove innovation efficiency should be noted. The importance of innovation efficiency becomes more obvious, where innovations toward more deregulated industries currently drive economic systems. It would not be wrong to claim that competition analyses have not based on two-dimensional static form anymore, but also other indicators like innovation. Therefore, innovation efficiency should not be ignored under all these conditions by considering the changing structure of economic development and consumer welfare. In this context, suppression of technology (controlling or deterring innovations) should be regarded as a direct violation of competition law.

3.2 Relevant patent theories on innovation suppression

IP rights give the owner exclusive rights, which may lead to deterioration of the competitive environment. Both IP and competition laws are directed towards the purpose of 'the wellbeing of EU citizens, businesses and society as a whole'[113] but they achieve this common goal in different ways. IP law encourages people to make innovations and encourages inventors to put on the market for enabling technological development.[114] Competition law, on the other hand, aims to provide a competitive environment and thus

[110] ibid 494.
[111] ibid 496.
[112] Whereas production efficiency addresses to 'increase social wealth over the whole range of output' and allocative efficiency addresses to 'increase social wealth only at the margin.' See Joseph Brodley, 'The Economic Goals of Antitrust: Efficiency, Consumer Welfare and Technological Process' (1987) 62 New York University Law Review 1020.
[113] Radostina Parenti, 'Competition Policy' (Fact Sheets on the European Union, 2020) <https://www.europarl.europa.eu/factsheets/en/sheet/82/competition-policy> accessed 14 March 2023.
[114] Nikolaos Zevgolis, 'The Interaction between Intellectual Property Law and Competition Law in the EU: Necessity of Convergent Interpretation with the Principles Established by the Recent Case Law' in Ashish Bharadwaj, Vishwas Devaiah and Indranath Gupta (eds), *Multi-dimensional Approaches Towards New Technology* (Springer 2018); Office for Harmonization in the Internal Market, 'European Citizens and Intellectual Property: Perception, Awareness and Behaviour' (Report, 2013) <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/25-11-2013/european_public_opinion_study_web.pdf> accessed 14 March 2023.

encourage the production of cheaper, higher quality, and innovative products.[115] Therefore, the suppression of innovation will bring adverse outcomes for both disciplines. The reason to include relevant patent theories in this section is to establish a basis of competition failures arising from the use of patent rights.

Amidst the Schumpeter-Arrow debate to set a legal ground for the IP rights, current expectations of competition law regarding the progress of technology are to encourage research activities through maximising incentives to innovate and maintain competitive markets where advanced technologies are easy to develop. However, it is quite hard to share this conventional opinion when technology suppression cases are considered. The likely way to contribute to the accepted opinion is to identify exceptional cases that impede the progress of innovation. Therefore, it is necessary to revisit some theories behind the grant of IP rights claimed by Kitch, Howells and Demsetz.

The Prospect Theory of patents proposed by Kitch mainly remarks on the social benefit of patents, which is the efficient coordination of technological development.[116] Therefore, the prospect function of patents is indicative of the public side of granting patent rights. This theory also integrates intellectual property into property rights successfully by providing temporary monopoly rights. This addresses a limited monopoly right to increase innovations as a consumer surplus.[117] From a different perspective, Howels argued that granting patents do not block technological developments, whereas practical difficulties in the administrative process cause the suppression of innovation.[118] He exemplified the Selden patent, which is known as a classical instance of the submarine patent. Selden, at the same time, is the name of the lawyer, who adapted a distinctive strategy somehow to protract the process of patent issuance and patent publication. For example, Selden used a patent, which was used in the automobile industry, for nearly 16 years with this tactic. The US took necessary measures afterwards and currently, a patent application in the US will be automatically published after 18-months from the earliest priority date,[119] where the EU also has the same timeframe.[120]

From a different viewpoint, Demsetz stated that patent systems provide a natural monopoly regulation. In such a way that, the existence of more than one undertaking to compete for getting an exclusive franchise implies a natural barrier for monopolists. This

[115] Ioannis Lianos, 'Some Reflections on the Question of the Goals of EU Competition Law' Centre for Law, Economics and Society Working Paper Series 3/2013 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2235875> accessed 14 March 2023.
[116] Edmund Kitch, 'The Nature and Function of the Patent System' (1977) 20 Journal of Law and Economics 265.
[117] John Duffy, 'Rethinking the Prospect of Patents' (2004) 71 The University of Chicago Law Review 439.
[118] John Howells, 'Patents and Downstream Innovation Suppression – Facts or Fiction? – A Critique of the Use of Historical Sources in Support of the Thesis that Broad Patent Scope Enables the Suppression or Hindrance of Downstream Useful-Technology Development' (5th International Conference on Innovation and Management, Maastricht, 10-11 November 2008) 163-180 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.490.9346&rep=rep1&type=pdf> accessed 14 March 2023.
[119] *Leahy-Smith America Invents Act* (US) [2011] 125 Stat 284, § 103 (e)(3).
[120] Convention on the Grant of European Patents (of 5 October 1973 as revised by the Act revising Article 63 EPC of 17 December 1991 and the Act revising the EPC of 29 November 2000) Article 93 (1)(a).

consequently maximises social benefit.[121] On the one hand, the prospect theory puts forward that the patent system effectively helps developing technology. Instead, it has an adverse effect by blocking or holding-up downstream innovations because elementary patents have general scopes as a consequence of first-mover advantage.[122] Therefore, specific measures ought to be taken for the passivation of suppressing innovations without discouraging innovators.

4 Reasons justifying impeding technological innovation

Impeding (suppressing) technology is more often the result of the introduction of a new technology being deliberately timed and presented to attempt to control the progression of technology due to commercial concerns. Hence, it is very rare to encounter a case of technology being directly suppressed for the sole purpose of suppressing; most instances of suppression show up because of business decisions. In other words, if interpreted broadly, technology suppression is a consequence of any event which halts or slows innovation or decreases research efficiency. In a narrower sense, it is possible to define technology suppression as keeping existing technology out of the market. However, although there are many practices likely to result in the suppression of innovation, this does not mean that all those practices are unlawful or anti-competitive. It is thus necessary to specify the problematic aspects of those practices rather than condemning all of them.

Saunders and Levine defined the suppression of innovation as the event that a patent holder both files to those patents and refuses to licence them in an anti-competitive manner. This practice suppresses technology because it prevents market competition and consumers from development. For example, an exclusive licensing agreement requires a patent holder to grant a licence for a specific undertaking by excluding other third parties. Any third party which does not have such a licence is precluded from developing existing technology, which again results in suppressing innovation. Abuse of patents is another means of suppressing innovation when it comes to patent consolidation (controlling competing technologies to disrupt innovation), patent pools (exploiting monopoly rights by gathering cross-licenses), patent thickets (obtaining a vast number of patents and thus leaving inventors in a difficult situation) so on and so forth. Not all these variations of patent abuse are strictly illegal, but they can be regarded as abusive if they stifle innovation.[123] Sometimes the market itself interferes with the proliferation of innovation. As explained in the previous chapter, for example, the network effect can increase the

[121] Harold Demsetz, 'Why regulate utilities?' (1968) 11 Journal of Law and Economics 55.
[122] Robert Merges and Richard Nelson, 'On Limiting or Encouraging Rivalry in Technical Progress: The Effect of Patent Scope Decisions' (1994) 25 Journal of Economic Behavior and Organisation 1.
[123] Kurt Saunders and Linda Levine, 'Better, Faster, Cheaper – Later: What happens when technologies are suppressed?' (2004) 11 Michigan Telecommunications and Technology Law Review 23, 54.

number of technologies being used, but newer technologies may nevertheless be overshadowed by current technologies, as was the case with the Dvorak keyboard.[124]

Some products may be presented as a bundle consisting of different tools with different functions, some of which may be produced by rival companies; this may force manufacturers to use certain specific technologies while prohibiting them from using others.[125] The process of standardisation is the effort to make products compatible while also providing an important market position for an undertaking having a specific technology, and consequently ensuring the profitability of and intellectual rights pertaining to a specific product. Dominant undertakings can set de facto standards to distort competition. However, it is also possible to use such standards to delay the introduction of innovations or avoid the use of a specific technology. This ultimately stifles innovation because companies are not compensated for their investments (sunk costs) unless their products conform to current standards.[126]

In addition to Article 102 TFEU and the TFEU-related patent issues explained above, agreements made between competitors to avoid using a specific technology and to each other's research area can be evaluated according to the terms of Article 101 of the TFEU. It is very difficult to determine how unlawful these practices are under the theory of harm, even though they clearly and explicitly halt the progression of innovation. In this regard, it is useful to refer to US antitrust law with the decision on tobacco companies by the Washington Superior Court in 1996. The court fined related tobacco companies for violating US antitrust law by "suppress[ing] independent research on the issue of smoking and health" regarding research on developing safer cigarettes. This fine was imposed because the companies in question were found to have suppressed new innovations to make cigarettes safer with less harmful ingredients.[127] The primary concern of such companies was their fear of the disruptive effects safer cigarettes would likely have on the conventional cigarette market. Before this decision, in the 1950s, there was another case involving the effort to create safer cigarettes. Liggett & Myers Tobacco Company has subsequently initiated a project ('Project XA') to create a cigarette which would be less dangerous to smoke in the 1970s. Therefore, the link between cancer and smoking has already been demonstrated by the time the project began and was ostensibly the reason the project was created. However, following this project, Philip Morris, the biggest cigarette manufacturer in the market, menaced Liggett & Myers on the grounds circulating negative information on the health effects of cigarettes would breach the industry agreement by damaging cigarette sales. Liggett & Myers was the first company to admit that cigarettes could cause cancer. The rest of the manufacturers cooperated in an effort

[124] Paul David, 'Clio and Economics of QWERTY' (1985) 75 The American Economic Review 332.
[125] Flynn (n 109) 512-3.
[126] Saunders and Levine (n 123) 49.
[127] *State of Washington v American Tobacco Co.* (1996) No-96-2-15056-8.

to suppress scientific evidence showing the causal relation between smoking cigarettes and cancer pursuant to their limited research.[128]

Overall, the above instances show how indirect and easily disguised efforts to suppress innovations can be. There are other practices that can be used to suppress technology including refusal to license, creating a patent pool or patent thickets, taking over rivals or bringing baseless suits for patent infringements. It is, therefore, necessary to set limits on practices which could be used to suppress innovation, which at present are normalised and even ignored. This issue is directly linked to the daily extension of the scope of patentable goods and processes. Patent protections are currently provided for everything from business methods to gene sequences; although it is thought expanding such protections even further will drive further innovation, its effects on the public interest are controversial in terms of the future impacts of technology suppression.[129] In other words, a new business is always at risk for patent infringement because a product or production method may always give rise to a conflict with the owner of a patent. Hence, the scope of a patent ought to be sharply limited in such a way that it serves the purpose of protection.

4.1 The lawfulness of innovation suppression practices

Saunders and Levine define technology suppression as the shelving of an invention, which is just as instrumental as its existing equivalents that other manufacturers will integrate if they are aware of this invention. Hence, the technology will be suppressed given the patent holder decides non-use or non-diffuse for controlling the advanced technology.[130] The lawfulness of suppression practices as anti-competitive tactics ought to be revisited as it directly affects the public interest. In addition to the safer cigarette case, there are other claims concerning the invention of the cancer cure and other diseases point out that the suppression of innovation is an actual and continuing phenomenon. Concerning the innovation suppression, it has to be regarded from two distinct sides, rather than trying to find common ground as Saunders and Levine proposed.[131] The intention behind to shelve an innovation identifies this adversary sides. First, it should be always bear in mind that a bona fide may be behind the practice of suppressing innovations whenever the patented invention is not profitable to be marketed or also, the invention cannot be patented because of their very natures. These states of affairs do not directly indicate any interruption of technological merit. On the contrary, indeed, businesses may suppress innovation on purpose with particularly reductive

[128] Saunders and Levine (n 123) 28-30.
[129] ibid 35-7.
[130] Ibid 25.
[131] ibid 25-6.

reasons, and only monopolies can put this strategy into practice as proved by economists.[132]

Businesses are making profits by using their monopoly rights to compensate sunk costs and to fend off free riders, which watch for an opportunity of imitating the protected product. This is also the aim of granting patents. However, the patent system prompts concern in terms of increasing more suppression of innovation because monopolies have tendencies to maintain the status quo.[133] It is more than likely that dominant businesses resort to suppressing their patented technologies, which create market entry barriers. Therefore, the patented but suppressed technology provides the patent owner with an opportunity of being a monopoly in a certain amount of time. It should be noted that it is anti-competitive to abuse the monopoly position, not having the monopoly position. In this matter, the suppression of innovation practices should be considered as anti-competitive because the patent owner decides to suppress his innovation and not allow others to use the innovation. This blocks existing rivals from commercialising the technology in both upstream and downstream markets.[134] It consequently indicates a violation of Article 102 TFEU.

Albeit the strong theoretical ties between the suppression of innovation and Article 102 TFEU demonstrated so far, there are more complex issues regarding the enforcement of competition law. In practice, the prejudgement that the patent is private property rather than a publicly granted privilege ties courts up in knots.[135] In regard to competition law litigation on the suppression of innovation, it seems that the only way to handle this issue by the court is referring to the intention of businesses. Irrespective of motivations, the court presumably will not find any competition law violation. Therefore, as a remedial suggestion, the legal-economic reasoning ought to be presented if patent protection is not requested for a marketable invention. Therefore, related conduct may be deemed reasonable if the business proves 'a technological necessity justification.' Hence, it seems that competition law should include an emphasis on suppressing competing technologies. Although the assumption of competition law addresses that maintaining a competitive process maximises innovation.

4.2 What if technologies remain unpatented?

As explained, the usual story concerning the suppression of innovation will likely begin after the obtainment of a patent right. However, it is not a rare occasion to remain inventions unpatented if they contain confidential business information, so-called trade secrets. Provided that businesses having trade secrets can exploit their invention as long

[132] Richard Gilbert and David Newberry, 'Preemptive Patenting and the Persistence of Monopoly' (1982) 72(3) The American Economic Review 517; Jean Tirole, *The Theory of Industrial Organization* (The MIT Press 1988) 393.
[133] Saunders and Levine (n 123) 44-5.
[134] ibid 42.
[135] ibid 41.

as they can keep it hidden absent any time limit. However, this may end up with happening of the risk (disclosure of the secret) that seriously jeopardises the secret owner. The tricky question is whether to obtain or not to obtain a patent is more rewarding because trade secret owner can make more profit without time constraint in case that secrets are kept. The unpatented formula of Coca-Cola becomes one of the most intriguing *cause célèbre* in this regard.[136] One can argue that it is possible to intervene in this secret based on innovation efficiency claims to develop healthier (and cheaper) forms of Coca-Cola, as it was the case with safer cigarettes. However, it would be an extreme example to coercively include this entirely different scenario into the suppression of innovation.

5 Conclusion

This paper provided a theoretical argument that practices impeding innovation have anti-competitive features and need to be treated by Article 102 TFEU in the context of EU competition law. For doing this, the current standpoint of the EC on innovation was specified by historical, theoretical, and practical perspectives. The analysis was started with illustrating fundamental theories of competition law developed by Chicago and Harvard schools. Although these two schools have had influences from time to time, the sui generis nature of EU competition law in line with the ordo-liberalist approach (on the protection and operability of the European common market as well as consumer welfare) was observed. Above all, it was demonstrated that the EC has gradually extended its interpretation in Article 102 TFEU to implement its political and economic policies towards making relations of competition and innovation more 'tangible'. In this context, the EC's more economic approach has brought itself in a more dynamic form, which helps to understand ever-changing market conditions. However, no initiative has been taken from either the EC or European courts to analyse competition in innovation, therefore R&D markets, even though they showed a tremendous effort when analysing innovative capabilities in merger cases.

There is a great deal of ambiguity surrounding the lawfulness of business practices suppressing innovation alongside the degree to which businesses contribute the technological development. This issue was examined throughout the study by analysing the EC's current approach to innovation. It was consequently illustrated that innovation considerations have not influenced judgements so far although the promotion of innovation was repetitively mentioned in both EU-level documents and case law. Instead, the progress and promotion of innovation were considered as offering wider choice for consumers. Then, it was critically argued the necessity to independently assess R&D markets, where competition in innovation occurs, as innovation has great importance on

[136] Yee Chin, 'Unilateral Technology Suppression: Appropriate Antitrust and Patent Law Remedies' (1998) 66 Antitrust Law Journal 451.

market power, specifically technology-driven markets. This importance was also underlined by showing the reasons why businesses attempt to suppress technologies.

Finally, this study showed the IP law's (specifically patents') important role for the disclosure and diffusion of innovations, which are also expected outcomes of EU competition law. Hence, the common and complementary grounds of these two legal fields were addressed to examine the issue of innovation suppression by visiting relevant theories. Flynn's quadripartite analysis was addressed to conceptualise the anti-competitive characteristics of suppression innovation practices. Therefore, it was concluded that competition policies should be designed to increase allocative, productive and innovation efficiencies (despite the difficulty to prove innovation efficiency with counter-factual analyses). In this context, Saunders and Levine suggested short and long terms deterrents about technology suppression. In the short term, contractual provisions may work, but in the long term, there is a need for radical changes in technology policies and existing laws (in addition to compulsory licencing, etc.).[137] However, they stated without hesitation that competition law enforcement should be directly applied when it comes to technology suppression, which is inherently anti-competitive as it harms consumers by preventing the disclosure of innovations.[138]

[137] Saunders and Levine (n 123) 64-5.
[138] ibid 68.

Marco Vargiu*

REVITALISATION OF THE ESSENTIAL FACILITIES DOCTRINE IN EU COMPETITION LAW

The complementarity with the new Digital Markets Act

Abstract
In recent years, platform economy has been raising competition concerns around the globe. In the European Union, the European Commission and the National Competition Authorities actively enforced Article 102 TFEU, sanctioning companies for abuse of a dominant position. Within the various theories of harm presented and mostly upheld by the Court of Justice, a common point is the ability of dominant undertakings to leverage, due to owning a platform, their market power in adjacent markets. This article therefore explores whether the Essential Facilities Doctrine should be revitalised to preserve a competitive structure and avoid exploitation of users. Moreover, the entry into force of the *Digital Markets Act* led researchers to analyse similarities with the doctrine and their possible complementarity once the Regulation will start applying in 2023. With a view to this possibility, concerns as to respect of the fundamental principle of *ne bis in idem* have been underlined, trying to clarify the future Competition Law landscape.

JEL CLASSIFICATION: K21

SUMMARY

1 Introduction

In recent years, the fast-growing platform economy captured the attention of the Antitrust Authorities, which intervened to restore competition several times in the context of abuse of a dominant position.[1] Specifically, the European Commission, under the guidance of Margrethe Vestager, sanctioned the most powerful US companies, notably GAFAM,[2] for various anticompetitive conducts considered to violate the principle of

* Law graduate, European Legal Studies, University of Turin
[1] Article 102, Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C 326.
[2] This acronym refers to Google, Apple, Facebook (Meta), Amazon and Microsoft.

competition *on the merits*.[3] These cases have been at the core of a heated debate among antitrust lawyers for several reasons. Firstly, they considered the innovativeness of the market definition in digital markets. Notably, their peculiarity leads Competition authorities to consider, in their investigation, features such as the various market facets, the networks effects, the economies of scale and scope, moving away from a traditional definition of market.[4] Secondly, the EU Commission presented new theories of harm, for instance the so-called self-preferencing in *Google and Alphabet v. European Commission* (Google Shopping),[5] in order to re-establish market competition. However, all cases have in common that owning a platform enables dominant undertakings to maintain and increase their market power in upstream and downstream markets. For this reason, a revitalisation of the Essential Facilities Doctrine, developed in the United States in 1912 in *Terminal Railroads,*[6] under the *refusal to deal* theory of harm, seems relevant. Indeed, it allows us to consider a platform as an Essential asset indispensable in order to compete in the market and, if necessary, to impose a duty to give access on the dominant undertaking. Moreover, a revitalisation of this doctrine reflects the lively debate around EU Competition Law goals: specifically, whether social values such as fairness and equality should be considered, as frequently evoked by the European Competition Authorities.[7] The new Regulation, which applies without prejudice to Article 102 TFUE, implies future intersection with the Essential Facilities Doctrine and its desirable enforcement. Consequently, an analysis of how the ex-ante regulation and the ex-post application of the Essential Facilities Doctrine might interact, considering recent developments in legal doctrine and case law, is the primary goal of this article.

The paper is structured as follows: the second paragraph presents a recap of the Essential Facilities Doctrine development in European Union competition case law. The third paragraph analyses the doctrine's applicability in digital markets, considering recent

[3] The concept of competition on the merits emerged in Court of Justice case law following the AKZO case. Since then, it helps Competition Authorities in investigating dominant undertakings' conducts. Specifically, the behaviour of dominant undertakings is considered part of the competition process when, by improving its efficiency and performance, it increases consumer welfare. Differently, the conduct is considered to infringe competition on the merits when the dominant undertaking's behaviour leads to exclusion of similarly efficient competitors, reducing consumer choice and violating Article 102 TFUE. See Case C-62/86, *Chemie BV v Commission of the European Communities* [1991] ECR I-03359; see also Aldo Frignani and Stefania Bariatti, *Treaty on Commercial Law and Public Economic Law, Competition Law in the EU* (vol 64, Cedam 2016) 275, 276.

[4] For this reason, the EU Commission presented a draft for a revised Market Definition Notice that fits better with the features of the digital economy, especially giving emphasis to non-price elements and new guidance in relation to market definition in multi-sided markets. See also: Commission Notice on the definition of the relevant market for the purpose of Community competition law [1997] OJ C372/5, 13.

[5] Case T-612/17, *Google and Alphabet v Commission (Google Shopping)* [2017] OJ C24/25.

[6] *United States v Terminal Railroads Association* (1912), 224 U.S. 383.

[7] The European School of Thought has always been moved by social values alongside economic goals. Specifically, even under the more economic approach and the implementation of a consumer welfare standard introduced in the United States after the Chicago revolution, EU Competition Law remained multi-valued, by protecting, as well as competitive process and market structure, also freedom of choice and fair distribution of wealth. See Ariel Ezrachi, 'EU Competition Law Goals and the Digital Economy' Oxford Legal Studies Research Paper 17/2018 <https://ssrn.com/abstract=3191766> accessed 29 March 2023.

case law. The fourth paragraph introduces to the Digital Markets Act and its similarities with the Essential Facilities Doctrine.

2 The Essential Facilities Doctrine development and the *Bronner* Test

Companies are traditionally free to choose with whom, when and under which conditions to deal with competitors. However, in some circumstances, the ownership of certain assets can represent a competitive advantage over competitors going beyond competition on the merits. Specifically, these assets can be essential to compete in the downstream or upstream markets. The refusal to give access, or the unfair conditions to use them, can undermine the competitive process and lead to elimination of the actual and *potential* competitors.[8] In the great majority of cases where the Essential Facilities Doctrine was applied, during the investigation, the Commission identified two relevant markets. The primary market, or upstream market, is where the undertaking owning the facility in question has a dominant position which grants it the possibility to act unilaterally without losing its market power, excluding competitors and exploiting consumers.[9] Notably, in the upstream market, the dominant undertaking owns the facility to which the competitors want access; for instance, in *Commercial Solvents v Commission,*[10] the cornerstone of the refusal to deal *theory of harm*, the dominant undertaking refused to provide the raw material (amino butanol) necessary to produce other chemical products. In this way, the dominant undertaking reserved for itself also the production of other products, *leveraging* its market power in the downstream markets.[11] Moreover, it is necessary to specify that two different situations can occur during the definition of the primary market. Firstly, the situation when the dominant undertaking supplied the product considered an essential facility for some time, then stops supplying it. In this case, the existence of a primary market is undeniable, as in *Commercial Solvents.*[12] In the second scenario, the dominant undertaking has always supplied the product together with the production outcomes. In this context, the Court of

[8] EU Competition Law considers abusive not only practices excluding present competitors in the relevant market but also practices which, by rising the barriers to entry, might limit the entry of potential competitors. See Communication from the Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings' [2009] OJ C 45/7.

[9] In the United Brands Company 1978 case, the Court provided the percentages of market share indicating a dominant position. Specifically, between 85% and 95% there's no doubt about the undertaking's dominant position; between 50% and 85% a dominant position is presumed, and this presumption is reversible; between 10% and 50% the Court made reference to other criteria, notably: the existence of a barrier to enter the market; the technological advantage of the undertaking in comparison to its competitors; down to 10% of market share there's a presumption of non-dominant position. See Case 27/76, *United Brands Company and United Brands Continentaal v Commission of the European Communities* [1978] ECR 1978-00207. Case 85/76, *Hoffmann-La Roche & Co AG v Commission of the European Communities* [1979] ECR 1979-00461.

[10] Cases 6-7/73, *Commercial Solvents v Commission* [1974] ECR 1974 -00223.

[11] Niamh Dunne, 'Dispensing with Indispensability' (2019) LSE Legal Studies Working Paper 15/2019 <https://ssrn.com/abstract=3476938> accessed 29 March 2023.

[12] *Commercial Solvents v Commission* (n 10).

Justice specified in *IMS Health*[13] that the two markets can be identified in the two stages of production and the upstream market can be a hypothetical one.[14] In defining the secondary market, it is fundamental to differentiate between the product and the one offered by the dominant undertaking in the primary market. However, in cases where the essential assets are not tangible products and protected by IP rights, different criteria have been elaborated by the Court of Justice to consider the refusal as an abuse of dominant position, notably the new product test established in *Magill.*[15]

The doctrine has been applied to different economic sectors, showing its versatility and utility to restore competition in both the relevant markets. Specifically, we can think of the cases *Port of Rodby*[16] and *Sea Containers v Stena Sealink,*[17] where the ports were the essential facilities; *Magill,*[18] where the information about television programs was indispensable to provide the weekly guide, or *Telemarketing*[19] in the advertisement market. During its development, the Court of Justice elaborated in *Bronner*[20] the conditions for the application of the doctrine, which, however, are not required under certain circumstances. Specifically, when, as held by the Court of Justice in *Slovak Telekom*[21] and *Lithuanian Railways,*[22] an *ex-ante* Regulation already prescribes the obligation of the dominant undertaking to give access to the facility, the remedies are not *structural* but consist in a cease-and-desist order from the conduct, and the facility is funded through public investments. Nevertheless, it is important to analyse the different conditions set by the Court of Justice in *Bronner*, as this enables us to assess their applicability to digital markets. On the other hand, it is necessary to remember that the recent EU Commission's practice and Court of Justice case law seem to treat them as a *lex specialis*.[23]

Firstly, it is necessary that the asset is considered indispensable for competitors and its reproduction is not feasible. In this context, the input is indispensable when no actual or potential substitutes are present in the market, as stated in *Magill*;[24] differently, when an alternative is present the conduct cannot be considered abusive.[25] For instance, in

[13] Case C-418/01 *IMS Health GmbH & Co KG v NDC Health* [2004] ECR I-05039.
[14] Anastasios A Antoniou, 'The Essential Facilities Doctrine Before the European Community Courts: Ostracized or Expanded?' (2010) 11 Cyprus and European Law Review <https://ssrn.com/abstract=1641125>.
[15] Joined Cases C-241/91 P & C-242/91 P *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission (Magill)* [1995] ECR I-743.
[16] Decision 94/119/EC, *Port of Rødby* [1994] OJ L 55/52.
[17] Decision 94/19/EC, *Sea Containers v Stena Sealink* [1994] OJ L 15/8.
[18] *Magill,* (n 15).
[19] Case 311/84 *Télémarketing (CBEM) v SA Compagnie luxembourgeoise de télédiffusion (CLT) and Information publicité Benelux (IPB)* [1985] ECR 1985-03261.
[20] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint GmbH & Co. KG* [1998] ECR I-07791.
[21] Case C-165/19 P *Slovak Telekom v European Commission* [2021].
[22] Case T-814/17, *Lithuanian Railways v European Commission* [2020].
[23] Pablo Ibáñez Colomo, 'Indispensability, and abuse of dominance: from Commercial Solvents to Slovak Telekom and Google Shopping' (2019) 10(9) Journal of European Competition Law & Practice 532.
[24] *Magill* (n 15).
[25] Maurits J Michon, 'The essential facilities doctrine requirement of indispensability and access to vertically integrated gatekeeper online platforms for downstream competitors' [2020] LL.M. thesis, Utrecht University.

Bronner, the Court of Justice argued that the delivery scheme to which the undertaking wanted access was not essential to carry out the economic activity. Indeed, the purpose here is to protect the "*as efficient as the dominant undertaking*"[26] competitors, which, even when operating on the same scale as the dominant undertaking, will not have the possibility to reproduce the facility, being, in that way, eliminated from the market because of the refusal.[27] The impossibility of reproducing the facility can principally be the consequence of three barriers to entry, notably the economic barriers, the legal barriers, and the technical barriers. Starting from the economic barriers, we should consider capital costs and economies of scale. Moreover, as the *IMS Health*[28] case shows, the possibility that consumers do not want to switch to another default option is considered an economic barrier.[29] Also, legal requirements for the reproduction of the facility can represent an insurmountable barrier: alongside the IP rights for which the Court of Justice established the *new product test*, we can also have cases where a government authorization is necessary to reproduce the facility, as in the *ARA*[30] case. Nevertheless, the indispensability test assumes relevance in cases where the remedies to restore competition, in line with the EU Commission's decision in *Slovak Telekom,*[31] are proactive or structural, for instance prescribing the terms under which the access to the facility should be given.[32]

The second condition for the application of the Essential Facilities Doctrine is that the refusal to give access by the dominant undertaking leads to elimination of competition in the downstream market.[33] In *Commercial Solvents,*[34] the refusal to supply Zoja with the raw material leads to the elimination of the only producer of ethambutol in the internal market; in the same way, in *Telemarketing*[35] the undertaking was not able to provide its services without operating in the TV broadcasting market. The consequences will be exit from the market of the undertaking seeking access to the facility, reducing innovation in the markets and the freedom of choice of consumers, who will be tied to the dominant undertaking's product or service, with higher prices.[36] Furthermore, even prevention of

[26] Specifically, the efficient competitor test is used by the EU Commission to demonstrate that the competitor excluded from the market can effectively match the offer of the dominant undertaking. See Raphäel De Coninck, 'The as-efficient competitor test: some practical considerations following the ECJ Intel judgment' (2018) 4(2) Competition law & Policy debate.
[27] Dunne (n 11).
[28] *IMS Health GmbH* (n 13).
[29] ibid.
[30] European Commission Decision C 5586, Case AT.39759, *ARA Foreclosure* [2016] OJ C 432/6 6.
[31] *Slovak Telekom* (n 21).
[32] Ibáñez Colomo (n 23).
[33] Liyang Hou, 'The Essential Facilities Doctrine – What was Wrong in Microsoft?' (2012) 43(4) IIC-International Review of Intellectual Property and Competition Law 251.
[34] *Telemarketing* (n 19).
[35] *Commercial Solvents* (n 10).
[36] Hou (n 33).

merely potential competition, not based on the characteristics of the market at the moment of the investigation, can be considered as a violation of Article 102 TFEU.[37]

Additionally, when the Essential Facility is an intangible product covered by IP rights, the protection of competition shall be balanced with the protection of Intellectual Property Rights.[38] The *new product test*, established by the Court of Justice in *Magill,*[39] meets this need and should be applied separately from the Indispensability test, as sustained in *Ladbroke*.[40] However, in later developments, the necessity to set a higher threshold for the application of the doctrine led to consider that only in "*exceptional circumstances*" IP rights can be considered as an essential facility. Those exceptional circumstances correspond to the introduction of a new and innovative product into market concerns.[41] To be innovative, the product should satisfy consumer demand differently from the existing ones, increasing the demand and reaching new consumers.[42] The burden of proof of the existing demand for the new product is on the undertaking seeking access to the facility covered by the IP rights.[43] Indeed, in these cases a balance between the *special responsibility* of the dominant undertaking[44] and the protection of its *incentive to innovate* is even more important. In fact, on this ground Justice Scalia, member of the Supreme Court of the United States in *Trinko,*[45] rejected the doctrine maintaining that it reduces business acumen. On the other hand, the European approach towards the incentive to innovate test clearly highlights the Ordo-liberal School of Thought's influence on EU Competition Law. In fact, for Ordo-liberals IP Rights are an obstacle to the creation of contestable markets and to the European integration process.[46]

On the other side, there is evidence that in the long run, in highly concentrated markets, dominant undertakings continue to innovate leveraging their dominant position in different markets, outside the concept of competition on the merits, and engaging in killer acquisition. The Microsoft case can be placed inside this context, firstly for the acknowledgment that even merely technical developments are recognised as satisfying the new product test. Moreover, the Commission and the Court of Justice, considering the

[37] Case T-201/04, *Microsoft Corp. v Commission of the European Communities* [2004] ECR 2007 II-03601.
[38] Valentine Korah, 'The interface between intellectual property and antitrust: the European experience' (2002) 69(3) Antitrust Law Journal 801.
[39] *Magill* (n 15).
[40] Case T-504/93, *Tiercé Landbroke SA v Commission of the European Communities* [1997] ECR 1997 II-00923.
[41] Magill (n 15).
[42] Aristeidis Demiroglou, 'Essential Facilities Doctrine and Intellectual Property Rights: Approaches under the Competition Law' [2016] School of Economic, business administration & Legal Studies.
[43] Christian Ahlborn, David S Evans and A Jorge Padilla, 'The Logic & Limits of the Exceptional Circumstances Test in Magill and IMS Health' (2004) 28(4) Fordham International Law Journal 1109.
[44] The special responsibility of the dominant undertakings does not just entail to refrain from violating Article 102 TFEU, but also a positive duty to supply competitors when the input is necessary to compete in the market. See Case 322/81, *NV Nederlandsche Banden Industrie Michelin v Commission of the European Communities* [1981] ECR 1983 -03461, para 57. See also Wolf Sauter, 'A duty to care to prevent online exploitation of consumers? Digital dominance and special responsibility in EU competition law' (2020) 8(2) Journal of Antitrust Enforcement 406.
[45] Supreme Court of the United States, 305 F.3d 89, *Verizon Commc'ns, Inc. v Law Offices of Curtis V. Trinko* [2004].
[46] David J Gerber, *Law and Competition in Twentieth-century Europe: protecting Prometheus* (OUP, 1998). See also Korah (n 38).

incentive to innovate in *Microsoft*, recognised that at first competitors could be harmed. However, in the long run, it is possible that competitors innovate in the market and the adjacent ones will stimulate Microsoft itself to innovate. Consequently, it is relevant to underline that, rather than disruptive innovations which lead to the presentation of a completely new product and competition for it on the market, the European approach privileges competition on the market and the improvement of the already present products.[47]

Based on these assumptions, we can move towards the applicability of the Essential Facilities Doctrine to digital markets. Indeed, relevance is given to the cases that involved the dominant platforms, notably Google, Apple, Facebook, Amazon, and Microsoft. Therefore, considering the doctrine efficient means it preserves the structure of competition and creates fairer and contestable digital markets.

3 The doctrine's applicability to digital markets

The application of the Essential Facilities Doctrine in digital markets could be useful because it targets the competitive advantage held by dominant players, making it more difficult for them to abuse of their market power. In digital markets, platforms act as intermediaries between multiple sides, such as online marketplaces connecting sellers and buyers; specifically, we talk about multi-sided market.[48] Moreover, the presence of strong network effects, both direct and indirect, increases the *lock-in* of the consumers inside the platforms, limiting their freedom of choice. In this way, it will be difficult for consumers to switch to other platforms as the costs are too high to be sustained by users.[49] Furthermore, dominant undertakings manage, to offer their services, an incredible amount of data, which could constitute an indispensable asset to increase the accuracy and quality of services in the downstream market. Without access to them and unable to reproduce them, competitors in the secondary market will not be able to compete with the platform that owns a competitive advantage due to its position.[50] In particular, user data can be used by the gatekeeper to predict where to invest, for instance engaging in M&A of innovative start-ups and eliminating potential competitors.[51]

[47] Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' [2019] DP2019-028, TILEC Discussion Paper <https://ssrn.com/abstract=3371457> accessed 29 March 2023.
[48] Jean-Charles Rochet and Jean Tirole, 'Platforms competition in two-sided markets' (2003) 1(4) Journal of the European Economic Association 990.
[49] Notably, with switch costing we refer to the economical or technical limits faced by consumers in changing supplier. The situation when these costs cannot be faced by the consumer, and there is no interoperability between the competitors, will lead to the phenomenon known as lock-in, often seen in the data-driven market. As also underlined by the Italian Competition Authority (AGCM, AGCOM) Survey on 'Big Data' (2017).
[50] Maria Wasastjerna, *Competition, Data and Privacy in the Digital Economy, Towards a Privacy Dimension in Competition Policy* (Wolters Kluwer 2020).
[51] The acknowledgment of the diversion of dominant platforms from R&D to M&A of start-ups is one of the main reasons behind the adoption of the Digital Markets Act. In fact, as will be highlighted below, the Digital Markets Act seeks to stimulate innovation around the platform and imposes, at Article 14, the obligation to notify the Commission in case of

The case of *Microsoft*[52] perfectly shows how the doctrine can be applied to open-up digital markets. Specifically, Microsoft's refusal to disclose the interoperability information, considered indispensable for the competitors, had the objective of *leveraging* the market power from the upstream market of the Operating system, where Microsoft had a *super-dominant* position,[53] to the downstream market of the workgroup server operating system.[54] Concerning the reproducibility of the interoperability information, the European Commission specified that the economic costs and the time necessary to reproduce it were not sustainable for the competitors.[55] The information, as alleged by *Sun Microsystems Inc.*, was necessary to grant efficient works, for instance inside an office.[56] Consequently, the imposition on Microsoft of a duty to share was necessary to avoid an irreversible situation where consumers and developers found themselves *locked-in* in Microsoft OS.[57] The interoperability information was protected by IP rights; therefore, it was necessary to establish whether the competitors wanted to introduce a new innovative product. The threshold provided in *Magill*[58] has been considerably lowered from the requirement of a "*new product for which potential consumer demand exists*" to the introduction of potential technical development in the field, sustaining innovation on an existing product.[59]

The Court of Justice and the Commission, imposing the duty to share, paid attention to the fact that the incentive to innovate of the dominant undertaking will be damaged. In this context, justifying Microsoft's refusal, the market development depends on its ability to innovate. On the other hand, through the duty to share the interoperability information, the whole sector would have the possibility to innovate.[60] Furthermore, considering that in digital markets innovations occur in the early stages of their development, the imposition of the duty to share would grant the possibility to implement the existing products. In the light of Microsoft's intermediary position between app developers and consumers, the dominant undertaking was also sanctioned for tying.[61]

concentration. In this line, see Pierre Larouche and Alexandre DeStreel, 'The European Digital Markets Act: A revolution grounded on tradition' (2021) 12(7) Journal of European Competition Law & Practice 542. See also Autorité de la Concurrence, Bundeskartellamt, 'Competition law and data' (2016).

[52] Case T-201/04, *Microsoft v Commission of the European Communities* [2007] ECR 2007 II-03601.

[53] Joined Cases C-395/96 P and C-396/96 P, *Compagnie Maritime Belge SA v Commission* [1998] ECR I-3257, Opinion of AG Fennelly, para 137.

[54]The working server group are those basic infrastructures which allow, for instance workers in an office to disclose files, share printers and access other services in the network. See Graef (n 48).

[55] Claudia Koch, 'Incentives to Innovate in the Conflicting Area between EU Competition Law and Intellectual Property Protection - Investigation on the Microsoft Case' (Heft 108, 2011).

[56] Katarzyna Czapracka, 'Where Antitrust ends and IP Begins – on the roots of the transatlantic clashes' (2007) 9 Yale Journal 44.

[57] Anneleen Straetemans, 'The EU Microsoft Case - Not a soft Case' (2007) 44(4) Jura Falconis 578.

[58] *Magill* (n 15).

[59] James Killik, 'IMS and Microsoft Judgement in the Cold Light of IMS' (2004) 1(2) The Competition Law.

[60] Wolfgang Kerber and Claudia Schmidt, 'Microsoft, Refusal to License Intellectual Property Rights, and the Incentives Balance Test of the EU Commission' [2008] <https://ssrn.com/abstract=1297939>. See also: Nikolas Guggenberger, 'Essential Platforms' (2021) 24 Stan Tech L Rev 237.

[61] Specifically, the Commission decisions, alongside the sanction for the refusal, sanctioned Microsoft for tying the Media Player to the Operating System Windows.

Therefore, the application of the essential facility doctrine allowed targeting the competitive advantage given by the intermediary position and restore competition in the market. The same arguments arise for the most recent investigations.

Starting from Google, two judgments involved the company under European Competition law. In *Google Shopping*, the Court of Justice upheld the European Commission's decision to sanction the undertaking for abuse of a dominant position, ex Article 102 TFEU. The Commission argued that Google discriminated between the different competitors, in the *comparison-shopping service* market, listing its own service at the top of the results page and in a more attractive format. The anticompetitive practice has been labelled as *self-preferencing;* however, even in the judgment the Court of Justice held that the search engine represents a "*quasi-essential facility*".[62] Neither the Court nor the Commission applied the doctrine based on the absence of an outright refusal by Google to give access; however, even unfair and inequitable terms of access, amounting to a constructive refusal, can effectively foreclose the downstream market where competitors operate.[63] Access to the search engine on equal footing is indispensable for competitors to reach and offer their services to consumers; or, as in the present case, they will deviate to Google's comparison-shopping service. Referring to *Microsoft*,[64] the Court recognized the indispensability of the general result page of the upstream market, and the unfeasibility to reproduce it, as the network effects and the switching costs were already high. On the other side, the EU Commission's fulfilment of the *Bronner* conditions was not necessary, firstly because the Commission limited itself to indicating that the format of the page should respect the principle of non-discrimination, without engaging in prescribing how the firm should implement it.[65] Consequently, the remedy can be categorized as reactive, escaping the *Bronner* criteria, as sustained by the Commission referring to the Court's judgment in *Van den Bergh Foods*.[66] However, it could be easily argued that the respect of the principle requires a positive obligation rather than a cease-and-desist obligation on the firm in modifying the mode in which the results are presented on the results page.[67] Additionally, Google's *super-dominant* position[68] increases its special responsibility to treat competitors equally in the downstream market, even if it is

[62] *Google Shopping* (n 5). See also Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era' (2019) Report for the European Commission 7.
[63] Ibáñez Colomo (n 23).
[64] *Microsoft* (n 37).
[65] *Google Shopping* (n 5), paras 697-705.
[66] Case T-65/98, *Van den Bergh Foods Ltd v Commissio*n [2003] ECR 2003 II-04653, para 161.
[67] Ibáñez Colomo (n 23).
[68] The Concept of super dominant position was presented for the first time by AG Fenelly in *Compagnie Maritime Belge*. It describes the situation of a monopolist or quasi-monopolist that consequently has a stronger special responsibility in ensuring that its behaviours do not harm the competition in the market by eliminating competitors and strengthening its dominant position. For further specifications and the evolution of the concept of super-dominant position in the EU Court of Justice case law, see Alessia Sophia D'Amico and Baskaran Balasingham, 'Super-dominant and super-problematic? The degree of dominance in the Google Shopping judgement' (2022) 18(3) European Competition Journal 614.

in direct competition with them.[69] Additionally, even if the list and design introduced by Google do not have the intent to exclude competition, the conduct falls outside competition *on the merits.*[70]

Alongside this case, in *Google Android* the dominant undertaking was sanctioned by the European Commission in 2018[71] and this was partially upheld by the Court of Justice in September 2022.[72] The abusive conduct consisted in a series of *tying* practices of applications on Android Devices through the different licence agreements concluded with the manufacturers. Specifically, the Commission considered that Google tied the Google Search app with Play Store, not giving the possibility to pre-install Play Store, indispensable for consumers, if the manufacturer failed to pre-install Google Search and Google Chrome as well. The facts of this case seem to recall a refusal to give access to an essential facility, rather than tying two distinct products. Play Store is an indispensable application for consumers once they buy an Android device and at the same time for the app developers to reach their audience, monetize their application through advertisements, and ensure the transaction.[73] On the other hand, in order to be able to talk about *tying*, as described by the Commission's Guidance Paper,[74] it is necessary that a substantial number of customers would purchase the tying product without the tied one.[75] In this regard, the Court of Justice confirmed that the conduct falls outside the competition *on the merits,* highlighting the intention of the undertaking to leverage its market power,[76] as well as the fine imposed by the EU Commission, the highest competition fine ever imposed in the EU.[77]

The same concerns arise in relation to the App Store in Apple's investigation.[78] The terms and conditions imposed on app developers to operate in the App Store are unfair and discriminatory. Specifically, the prohibition to provide in-app purchases and the high commission fees increase costs for competitors and prices for users of the application. Furthermore, Apple engages in *self-preferencing* its application over competitors, as claimed by Spotify in the music streaming market. On top of this, the app developers

[69] Case T-203/01, *Manufacture française des pneumatiques Michelin v Commission of the European Communities* [2003] ECR 2003 II-04071.
[70] Denis Lylian, 'New chapter in the Google Shopping saga', n 0032, Competition Forum, 2022 <https://competition-forum.com/new-chapter-in-the-google-shopping-saga/>.
[71] *Google Android* (Case AT.40099) Commission Decision [2019] OJ C 402 2019, 19.
[72] Case T-604/18, *Google and Alphabet v Commission (Google Android*) [2022].
[73] Pinar Akman, 'A preliminary assessment of the European Commission's Google Android decision' [2019] CPI Antitrust Chronicle December.
[74] Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ C 45/7.
[75] Graef (n 48).
[76] *Google and Alphabet* (n 72).
[77] Akman (n 73).
[78] Press release 'Antitrust: Commission opens investigations into Apple's App Store rules' 16 June 2020 IP/20/1073.

which offer *digital goods and services*[79] are affected by the 30% commission fees and cannot include external links for purchasing goods and services outside the App Store, otherwise they can be excluded from the platform. The App Store is an indispensable asset for app developers: without it they cannot reach the iOS users and thus give up a large part of the market. The consequence of the application of these unfair conditions is highly harmful to the competition structure and innovation in the market.[80] In this context, the fulfilment of the *Bronner* test will not be necessary as access to the App Store is granted by the dominant undertaking. However, the case of *Epic Games*[81] perfectly shows how unfair terms and conditions, and eventually their violation, can lead to delisting the app developers from the App Store.[82] In these cases, the assessment of the indispensability of the App Store to reach the various sides of the market implied considering the economic unfeasibility of reproducing the App Store.

Equally, the data acquired by dominant platforms on the various sides of the markets, from business and consumer users, enable them to adjust their investments, offer better services and outcompete their rivals in the downstream markets. Moreover, as under the GDPR[83] data can be categorized as *voluntary-given* data and data acquired through *observing* the users' behaviours in surfing the internet, there is a possibility that the data controller engages in exploitative practices outside the competition *on the merits*.[84] Their exclusive ownership, considering their importance, can lead to the elimination of *potential* competition and increase barriers to entry. Both at the European and National level, principally in the social networks market, Competition Law enforcers launched a series of investigations over *Facebook*, now Meta.[85] The dominant platform, thanks to its intermediary position, can acquire more information about the interest and behaviour of users, considerably increasing its turnover in the advertisement market.[86] Furthermore, the personalised services offered to the users will increase their dependence on the ecosystem, supplying the dominant platform with more data and creating a *feedback*

[79] This distinction is not justified by practical considerations and lacks clarity, for instance concerning online medical consultation, online lectures, and fitness classes. As to the former, the medical consultation apps, the problems around the definition of digital services arose in 2019 with relation to certain Chinese apps; in the end, Apple considered that they were not to be understood as digital services.
[80] B Kotapati and others 'The Antitrust Case Against Apple' [2020] <https://ssrn.com/abstract=3606073>.
[81] *Epic Games v Apple Inc*, 493 F Supp 3d 817 (N D Cal 2020).
[82] Damien Geradin and Dimitrios Katsifis,'The Antitrust Case against the Apple App Store' (2020) DP2020-035, TILEC Discussion Paper.
[83] European Parliament and the Council, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation (GDPR) [2016] OJ L 119, 1.
[84] The distinction, based on how they are collected, was presented in the Joint Report of the French and German Competition Authorities. Specifically, on the one hand data are collected after the owner's consent, in line with Article 7 GDPR, on the other hand data can be acquired by dominant undertakings even by simply analysing user behaviours in the platforms.
[85] Autorité de la Concurrence, Bundeskartellamt, 'Competition law and data' (2016). See also AGCM, AGCOM, 'Survey on "Big Data"' (2020).
[86] Andres V Lerner, 'The Role of "Big Data" in Online Platform Competition' (2014) SSRN Working Paper 41,44 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780> accessed 29 March 2023.

loop.[87] Indeed, those data will be indispensable for the competition in downstream markets where most of the time also the dominant platform operates and where the refusal will lead to the elimination of the *actual* and *potential* competition.[88] The definition of the two markets in these cases can be peculiar: considering that data are not traded, only a hypothetical upstream market might be identified. On the downstream market, the definition will depend on the products or services offered by the undertakings seeking access, for instance, the advertisers.[89] The indispensability of data could be assessed based on financial conditions, reasonable period and the ability of competitors to reproduce data; in line with Microsoft, their reproduction will be time-consuming, and the *lock-in* effect might have exclusionary effects.[90] The European Commission's investigation, launched on 4 June 2021, stresses this point, arguing that the combination of data from social networks and business users in the online classified ads market gives Facebook the possibility to outcompete them in the secondary market in favour of Facebook Marketplace.[91] Furthermore, the possibility to use data from the various sides of the market to operate in the downstream market is a competitive advantage. The vertical integration of Facebook increases these effects, as various data from API (Application Programming Interfaces) and the ones obtained by other services as WhatsApp and Instagram can be combined. This practice has been considered in the Bundeskartellamt's decision against *Facebook*[92] as an abuse of domination position ex Article 102 TFEU. While considering the exclusionary effects, the Competition Authority focuses on the exploitation of users and in particular the prescription that user content shall be freely given, specific, informed, and unambiguous ex Article 7 GDPR.[93] Indeed, the informational asymmetries between users and the platform as well as the restrictions on privacy are considered market failures.[94] However, based on recent case law, and in

[87] Inge Graef, 'Data as Essential Facility, Competition and Innovation on Online Platforms' (2016) KU Leuven Faculty of Law 248.
[88] On this point, the United States case for the refusal by Twitter is an example of the possibility to apply the doctrine to data. See *PeopleBrowsr, Inc et al v Twitter, Inc.* (*PeopleBrowsr*), C-12-6120 EMC, 2013 WL 843032 (N D Cal 6 March 2013) [1].
[89] *IMS Health GmbH* (n 13). See Pierre Larouche, *Competition Law and Regulation in European Telecommunications* (Hart Publishing 2000) 207, 212.
[90] Even if concerning contact details of customers, the decisions of the Belgian and French Competition Authorities underlined the indispensability of data to offer quality services which can compete with the dominant undertaking in the downstream market. See Autorite´ de la concurrence, Décision 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société´ Direct Energie dans les secteurs du gaz et de l'électricité. Belgian Competition Authority, Beslissing BMA-2015-P/K-27-AUD van 22 september 2015, Zaken MEDE-P/K-13/0012 en CONC-P/K-13/0013, Stanleybet Belgium NV/Stanley International Betting Ltd en Sagevas S.A./World Football Association S P R L /Samenwerkende Nevenmaatschappij Belgische PMU S C R L t Nationale Loterij NV 69-70.
[91] Press release, 4 June 2021, Antitrust: Commission opens investigation into possible anticompetitive conduct of Facebook.
[92] Bundeskartellamt's decision 6th Division, Case B6-22/16, *Facebook*, 6 February 2019.
[93] Article 7, General Data Protection Regulation (GDPR). See also Maria Wasastjerna (n 50) 148.
[94] Nicholas Economides and Ioannis Lianos, 'Restriction on privacy and exploitation in the Digital Economy: A competition law perspective'5 CLES Research Paper Series 4 (2019). See also, Marco Botta and Klaus Wiedemann, 'EU Competition Law vis-à-vis exploitative conducts in the data economy - exploring the Terra incognita' Max Planck Institute for Innovation and competition Research Paper 4 (2018).

particular the Opinion of AG Øe in *Slovak Telekom*, if we consider platforms indispensable it will not be necessary to refer to the *Bronner* test when the request comes from a user who is already in the business. On the contrary, if a third party requires access to the platform data, the anticompetitive effect of a refusal might refer to *Bronner*.[95]

Focusing on *Amazon* and its online marketplace, several investigations have considered the gatekeeper role of the dominant undertaking, both at National and European level. Firstly, the Amazon ecosystem is composed of the online marketplace, a two-sided market where buyers and sellers meet, and e-commerce, where the dominant undertaking offers its products.[96] The indispensability of the online marketplace is given by the impossibility in the modern economy for sellers to not use Amazon, otherwise they lose a large part of the demand for a product, especially where Amazon offers its *Amazon choice*.[97] Moreover, once sellers operate inside the online marketplace, several instruments to increase sales are essential to compete in it, among them Buy Box. In 2019 the EU Commission launched an investigation on the terms and conditions to access Buy Box and the competitive advantage owned by Amazon thanks to the data acquired in the upstream market of the online marketplace. Indeed, the competitive advantage can ensure the possibility to leverage the dominant position in the downstream market. Moreover, at Member States level, the Italian Competition Authority well identified that the conditioned access to the Buy Box, and other facilities, to the use of the Prime services enable Amazon to leverage its dominant position also in the logistic services market.[98] Therefore, the ownership of an indispensable asset, as the marketplace, enables the dominant undertaking to acquire market power, limiting the freedom of choice for users and excluding competitors in the downstream markets. Even in the case of Amazon, where the costs to start operating in the online marketplace are very low,[99] the unfair treatment and practices by dominant undertakings have the same exclusionary effects of a refusal to supply. As already highlighted above, even in this context the fulfilment of the *Bronner* conditions will not be necessary, as the access to the essential asset, the online marketplace, is granted under unfair terms which potentially will require a cease-and-desist obligation from the anticompetitive conduct.

In conclusion, this doctrine might be a potential tool in *ex-post* competition law enforcement, in order both to sanction and prevent abusive conducts. At the same time, in December 2020 the European Commission presented the Digital Markets Act,[100] to

[95] Daniel Mandrescu, 'Why you (often) don't need the essential facilities doctrine in the digital economy? – Interpreting Lithuanian Railways and Slovak Telekom' (Lexxion, 2020) <https://www.lexxion.eu/en/coreblogpost/why-you-often-dont-need-the-essential-facility-doctrine-in-the-digital-economy-interpreting-lithuanian-railways-and-slovak-telekom/> accessed 29 March 2023.
[96] Lina Khan, 'The Separation of Platforms and Commerce' (2019) 119 Colum L Rev 973.
[97] Guggenberger (n 60) 258.
[98] Italian Competition Authority (AGCM) decision A528, *Amazon* [2021].
[99] ibid.
[100] European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector, Digital Markets Act [2022] OJ L 265/1.

ensure *fairness* and *contestability*. Starting from the goals and moving to the obligations, the Regulation seems to recall the recent ex-post competition investigations described above. Moreover, considering the gatekeepers' duty to give access, prescribed by the Digital Markets Act obligations, will impact on the future ex-post case law of the Essential Facilities Doctrine.

4 The new *Digital Markets Act* and the Essential Facilities Doctrine: similarities and complementarity

The *Digital Markets Act*'s[101] goal is to ensure fairness and contestability through a set of obligations imposed on gatekeepers, under the formula of one size fits all, which tries to overlap the slowness of the ex-post competition enforcement.[102] Moreover, through structural and behavioural remedies it tries to stimulate the gatekeepers' respect of obligations. The huge fines imposed over the years, due to their huge turnovers, started to be considered by dominant platforms as part of the cost of doing business.[103] The question of whether the aim of ensuring fairness and contestability is encompassed in the European Competition policy, as ordo-liberal thinking would suggest,[104] is reflected on our question about similarities with the Essential Facilities Doctrine. Indeed, the DMA seeks to overcome the imbalance of power and informational asymmetries between platforms and users, especially in cases when the latter are indirect competitors.[105] As in the case of the Essential Facilities Doctrine application, the imposition of certain obligations over gatekeepers, a different concept of market power,[106] tries to redistribute value along the value chain. Redistribution is granted by restoring competition on a "*level playing field*", protecting competition as a process and free consumer choice, differently from what could happen if the intervention in the market was only moved by the consumer welfare standard,[107] by the well-known "*more economic approach*".[108] Under this perspective, the DMA seems to recall the social principles which are behind the Essential Facilities Doctrine

[101] Digital Markets Act, Recital 2.
[102] Monti (n 4).
[103] Nicolas Petit, 'The proposed Digital Markets Act (DMA): A legal and policy review' (2021) 12(7) Journal of European Competition Law & Practice 529.
[104] Manuel Wosdorfer, 'The Digital Markets Act and the E.U. Competition Policy: A critical Ordoliberal Evaluation', (2022), Maine Business School &School of Computing and Information Science.
[105] Petit (n 103).
[106] Damien Gerardin, 'What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a Digital Market Act?' (2021) <https://ssrn.com/abstract=3788152> accessed 29 March 2023.
[107] The consumer welfare standard was introduced by Robert Bork, principal exponent of the Chicago School of Thought. It oriented the Competition Authorities' intervention in high concentrated markets only when the total welfare, in the Wilson trade-off model, is reduced by the conduct under investigation. Historically, the consumer welfare standard in the European Union is interpreted as consumer surplus, confirming the redistribution goals of EU competition law: cf Robert Bork, *The Antitrust Paradox: A Policy at War with itself* (Basic Books 1978). See also Marktabgrenzung, 'Differences in Schools of Thought on protecting competition: Chicago School vs European School' (2016) 2 CCR - Competition Competence Report Autumn.
[108] Heike Schweitzer, 'The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal' (2021) 3 Zeitschrift für europäisches Privatrecht 503, 544.

and which were replaced under the Chicago School of Thought revolution, drifting away from the social aspect of Competition Law.[109] The DMA seeks, as the Essential Facilities Doctrine would, to neutralize gatekeeper conducts mainly made possible by owning the essential asset, which increases the dependence of end users and competitors on their platforms.[110]

4.1 Identification of gatekeepers and their core platform services

Analysing the regulation, it is necessary to specify that its definition of gatekeepers does not correspond to the traditional assessment of a dominant position under EU Competition Law.[111] This important difference is due to the acknowledgment of the peculiarities of digital markets and their main features: for instance, network effects and economies of scale and scope.[112] Furthermore, the regulation applies to those digital services, called Core Platform Services in Article 2 DMA, which are considered an "*important gateway*" for ancillary markets. In this way, the difficulties faced by Competition Authorities as to market definition, related to two-sided market and vertical integration, are outdated.[113] Normally, under the Essential Facilities Doctrine, after defining the market the Competition Authority must give evidence of the refusal to give access and the indispensability of the service concerned. Under the Digital Markets Act, it is already recognized that, even if there is no formal refusal to access the Core Platforms Services, the gatekeeper's position enables it to impose unfair terms and conditions on its direct and indirect competitors.

The Core Platforms Services list, Article 2 DMA,[114] encompasses Online Search engines, Online Social networks, Video-sharing platforms, Operating systems, Online intermediation services between consumers and businesses, Web Browsers, Virtual Assistants, Connected TV, and Cloud computing services. Moreover, the list is not closed to future updates, for which the ordinary legislative procedure must be respected, preserving the right of initiative for the European Commission after a market investigation, as established by Article 17. However, the procedure is criticised by scholars as it will result in a late update, as in the Competition Law *ex-post* enforcement.[115] Hence, it is relevant to underline that those services are implicitly recognized as indispensable to competition in the downstream markets. Furthermore, the threshold has been lowered as

[109] ibid. Further on the social side of the European Union competition law, See Ariel Ezrachi, 'EU Competition Law Goals, and the Digital Economy' (2018) 17 Oxford Legal Studies Research Paper.
[110] Pablo Ibáñez Colomo, 'The Draft Digital Markets Act: a legal and institutional analysis' (2021) 12(7) Journal of European Competition Law & Practice 561.
[111] Gerardin (n 106).
[112] ibid.
[113] Schweitzer (n 108) 503, 544.
[114] Digital Markets Act, Article 2. For a resume of the Regulation, cf Natalia Moreno Belloso, 'The Proposal for a Digital Markets Act (DMA): A Summary', <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3999966> (accessed 28 March 2023).
[115] Schweitzer (n 108).

the DMA does not refer to the CPS as indispensable, but as "*important gateways for business and end users to reach other end users*".[116] Therefore, it is assumed that an abuse in supplying those services, when the undertaking matches the definition of gatekeeper, leads to elimination of the *actual* or *potential* competition in the downstream and upstream markets, corresponding to the third condition established in *Bronner*[117] by the Court of Justice. However, in the potential ex-post enforcement of the Essential Facilities Doctrine it will be no longer necessary to fulfil the *Bronner* criteria to sanction dominant undertakings in the digital sectors, as they are already encompassed within the *ex-ante* regulation.

As to the definition of gatekeepers, the DMA considers the features of the digital economy. Specifically, it takes into consideration the quantitative and qualitative criteria listed in Article 3(2).[118] As well as applying the criteria of turnover and active user, as well as durable or foreseeable entrenched position, the Commission can consider the data-driven advantage of the undertaking, economies of scale and scope, lock-in and switching costs for users, vertical integration and its structural characteristics. Under the Essential Facilities Doctrine, this position refers to the actual or future "*unavoidable trading partner*" which refuses to deal.[119] However, the criteria used to identify gatekeepers are lower than the standards required establishing a dominant position, meeting the need of preventing the situation of abuse under Competition Law.

Once an undertaking is defined as gatekeeper, the obligations set out in the DMA apply under the formula of "*one size fits all*"; from certain viewpoints, they recall the Essential Facilities Doctrine, as will be illustrated in the next subparagraph.

4.2 Gatekeepers' obligations and the Essential Facilities Doctrine

Before comparing the obligations set out in the DMA and the remedies applied in the Essential Facilities Doctrine case law, it is necessary to point out the flexibility of the approach proposed by the DMA. Specifically, two categories of obligations are imposed on gatekeepers: the ones which are directly applicable, provided by Article 5,[120] and the ones which can require further specification by the European Commission, listed in Article 6.[121] Alongside them, transparency obligations are established in Articles 12 and 13 in light of

[116] Ibáñez Colomo (n 110).
[117] *Bronner* (n 20).
[118] Digital Markets Act, Article 3(2).
[119] Case 85/76, *Hoffmann-La Roche v Commission of the European Communities* [1979] ECR 461, para 41]; Case C-95/04, *British Airways plc v Commission of the European Communities* [2007], para 75; Case T-286/09, *Intel Corporation, Inc v European Commission* [2009] OJ C 220/41; T-155/06, *Tomra Systems ASA and Others v European Commission* [2010] ECR 2010 II-04361, para 269. *See* Alexandre de Streel and others, 'The European Proposal for a Digital Markets Act: A First Assessment' (2021) 11 CERRE-Report.
[120] Digital Markets Act, Article 5.
[121] Digital Markets Act, Recital 2, Article 6.

the killer acquisitions which in recent years strengthened gatekeepers' positions in digital markets.[122]

In line with the case law illustrated above, the obligations foreseen by the DMA can be categorized according to their objectives. Firstly, the obligations aimed at preventing the expansion of gatekeepers in ancillary markets,[123] and secondly the ones aimed at reducing barriers to entry for new potential competitors.[124] The analysis will highlight how the objectives pursued by the DMA are complementary, or almost identical, to the ones pursued by ex-post Competition Law enforcement.

Notably, we can refer to *Microsoft*,[125] where the European Commission intervention has the aim to avoid the *leveraging* of the dominant position, from the Operating system market to the working server group market, through the refusal to supply the interoperability information. The obligation to supply the interoperability information is now a DMA obligation, specifically in Article 6(7), and is susceptible to be further specified by the Commission, for which is not necessary to prove the negative effects in case of non-compliance.[126] On the other hand, considering the most recent case law, when gatekeepers grant the interoperability information but under unfair terms and conditions, in the ex-post competition assessment it will be not necessary to prove the fulfilment of the *Bronner* criteria. Additionally, as the interoperability obligation could be further specified, the Commission would have the possibility to define the level of mandatory interoperability which will be exempted from the indispensability test in the ex-post enforcement. Moreover, in *Microsoft,* the obligation imposed by the Commission avoided the elimination of *actual* and *potential* competition and the rise of excessive barriers to entry, which might lead to consumer *lock-in* and hamper innovation in the long run. In the same way, the DMA seeks to stimulate competition around the platforms, favouring the emergence of competitors in the downstream markets, which potentially can be direct competitors in the future.[127] As highlighted in the Commission Impact Assessment,[128] the DMA aims to stimulate innovation on the business user side of the market, as it has been noticed that most of the undertakings which are to be defined as gatekeepers have diverted from *R&D* to *M&A* of new entrants.[129]

The same can be highlighted concerning data. Firstly, the prohibition of combining data collected from the CPS with other personal data collected from other services, Article

[122] Belloso (n 114).
[123] The expression "ancillary market" is not clearly defined in case law. However, ancillary markets should be interpreted as markets which depend on the platforms, or which operate close to them. For instance, the logistic services market should be considered as ancillary to the online marketplace.
[124] Filomena Chirico, 'Digital Markets Act: A regulatory perspective' (2021) 12(7) Journal of European Competition Law & Practice 493.
[125] *Microsoft* (n 53).
[126] Schweitzer (n 108).
[127] Larouche and de Streel (n 51).
[128] European Commission Impact Assessment of the Digital Markets Act, 16 December 2020, <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-markets-act> accessed 29 March 2023 at 279.
[129] Schweitzer (n 108).

5(2)(b), secondly the re-affirmation of the right to data portability, Article 6(1)(9), and thirdly the right to access to aggregated or non-aggregated data for publisher and advertisers, Article 6(1)(8). Under these obligations, as maintained by the Bundeskartellamt in *Facebook,*[130] consumer exploitation is avoided. The purpose is to avoid that a dominant undertaking has the possibility to outcompete rivals only thanks to the amount of data processed. Moreover, the obligations also aim at unlocking the consumers' choice over their data and the way they are processed.[131] Hence, it should be noted that one of the main goals of EU Competition Law has always been the protection of the freedom of consumer choice, especially in the context of the EFD, where the obligation to share imposed on dominant undertakings aims at increasing or improving the quality of the options available to consumers.[132] In fact, as according to the EFD, an *ex-ante* obligation facilitates the entry of new competitors into downstream or ancillary markets and grants fair competition to the already present market actors, such as the *publisher* and *advertisers*, who through the data can do their verification on the CPS.

Furthermore, the DMA prohibits the gatekeeper to hold business users back from using a different payment system, Article 5(4). The prohibition recalls the EU Commission's investigation into Apple's[133] terms and conditions to operate inside the App Store. In fact, alongside the unfair fees imposed on developers wishing to offer their applications in the App Store, the dominant undertaking prohibited app developers from providing users with a different payment system outside the platform. The imposition of such obligation aims at granting developers access to the platform, indispensable for reaching consumer demand under fair and equitable terms.[134] In the same way, the application of the Essential Facilities Doctrine could impose fair access to the platform, avoiding its *envelopment* and the elimination of actual and potential competition.

Moreover, the prohibitions of *self-preferencing* and *tying*, respectively in Article 6(5) and Article 5(8), reflect the *Google* and *Amazon* cases, both at European and National level. Specifically, the obligations impose on the gatekeeper the duty to grant users the possibility to uninstall the pre-installed application: this is the same result of the *Google Android*[135] judgment, presented as *tying*. Additionally, for the self-preferencing prohibition, we can refer both to *Google Shopping*[136] and the case of *Amazon*[137] before the Italian Competition Authority. In these cases, the ownership of the indispensable CPS

[130] Bundeskartellamt, *Facebook* decision (n 92).
[131] Rupprecht Podszun, Philippe Bongartz and Sarah Langenstein, 'Proposal on how to improve the Digital Markets Act' (2021) 2 <https://ssrn.com/abstract=3788571> accessed 29 March 2023.
[132] Paul Nihoul, 'Freedom of Choice: The Emergence of a powerful concept in European Competition Law' (2012) 3 Concurrences Review 54, 70.
[133] Press release: 'Antitrust: Commission opens investigations into Apple's App Store rules', 16 June 2020, IP/20/1073.
[134] Bapu Kotapati and others, 'The Antitrust Case Against Apple' (2020) <https://ssrn.com/abstract=3606073> accessed 29 March 2023.
[135] *Google Android* (n 71).
[136] *Google Shopping* (n 5).
[137] Amazon, Italian Competition Authority (AGCM) decision (n 98). European Commission Press Release IP/19/4291, Antitrust: Commission Opens Investigation into Possible Anti-Competitive Conduct of Amazon [2019].

allows the dominant undertakings to divert consumers to use their ancillary services, such as *Amazon Prime* logistic services, leveraging their dominant position in adjacent markets.

Consequently, several similarities can be found between the doctrine and the DMA; on the other hand, the latter goes further and allows for behavioural and structural remedies to be imposed[138] in case of non-compliance. Alongside fines, which in case of non-compliance can reach, for three times in 8 years, 20% of the global turnover, structural remedies can be imposed, such as a ban on the acquisition of other businesses. Scholars in this context have advocated for the introduction of more structural remedies, since fines are understood by gatekeepers as a cost of doing business, especially for GAFAM.[139]

However, we should specify that even with the several similarities between the DMA, which applies *ex-ante*, and the Essential Facilities Doctrine, this does not impede the application of the latter in *ex-post* Competition Law enforcement. In fact, the DMA applies without prejudice to the application of Article 102 TFEU, as specified in Article 1 (6). Consequently, the same conduct could be a violation of both EU Competition Law and DMA provisions. Therefore, future intersection between the *ex-ante* regulation and the *ex-post* intervention might raise concern about the respect of the *ne bis in idem* principle, as addressed in the next paragraph.

4.3 Revitalisation of the Essential Facilities Doctrine and implementation of the DMA: *ne bis in idem* principle

The application of the Digital Markets Act does not affect the enforcement of EU and National Competition rules. Starting from this assumption, the same conduct, here the refusal to give access to an essential facility, could be a potential object of three different cumulative proceedings. However, Article 50 of the Charter of Fundamental Rights of the European Union,[140] which encompasses administrative fines, states that an undertaking cannot be sanctioned for the same conduct under different proceedings. The principle has been the object of extensive case law before the Court of Justice, which recently intervened for the purpose of defining how the "idem" condition shall be interpreted under Competition Law. Indeed, as presented by AG Bobek,[141] two relevant interpretations of the idem condition exist. On the one side, the so-called "*idem crimen*" approach, which considers the idem condition fulfilled when the proceedings concern the same natural or legal person, the same facts, and protect the same legal interest. Differently, under the "*idem factum*" approach the protected legal interest is not relevant, thus the application of the fundamental principle is broadened. In the field of EU Competition Law, the Court

[138] Podszun, Bongartz and Langenstein (n 131).
[139] ibid. In this part of the DMA, the ordo-liberal influence is particular evident. In this line see Eucken, 'El Problema Político de la Ordenación' in Lucas Beltrán (ed), *La Economía de Mercado. Vol I* (Sociedad de Estudios y Publicaciones 1948).
[140] Council of the European Union, Charter of Fundamental Rights of the European Union (2007/C 303/01) [2007], C 303/1.
[141] Case C-117/20, *bpost SA v Autorité belge de la concurrence*, Opinion of AG Bobek [2021].

of Justice historically opted for taking the legal interest protected in the two proceedings into consideration as well, as in *Slovak Telekom*[142]. However, in *bpost*[143] and *Nordzucker,*[144] the Court of Justice followed the idem factum approach, specifying that the principle is violated when two proceedings sanction the same natural or legal person for the same conduct, the legal interest protected by the proceedings being irrelevant. Nevertheless, the presence of two proceedings could be justified by Article 52 (1) of the Charter[145]. In fact, when the duplication is provided by law, under different legislations which pursue different legal interests, there is no violation of the principle if the measures are proportionate and necessary to pursue their objectives.[146] As specified in the DMA, the sector regulation pursues a different but complementary role to Competition Law enforcement.[147] On the other hand, it is undeniable that, thanks to the ordo-liberal influence,[148] EU Competition Law does not pursue only economic objectives. Indeed, values such as fairness and the creation of contestable markets are at the centre of Competition Law enforcement, especially in recent years under the guidance of EU Commission Vice-President Margrethe Vestager.[149] Under this assumption, the only choice for a legal basis is Article 114 TFEU,[150] with the goal of harmonising the regulation of digital markets among Member States, which could entail a different legal interest.[151]

Analysing the risk of violating the *ne bis in idem* principle, two different situations deserve attention. Firstly, when a competition *ex-post* enforcement, hypothetically under the Essential Facilities Doctrine, is opened by the European Commission and at the same time the undertaking, defined as gatekeeper, is sanctioned for non-compliance with DMA obligations.[152] This scenario is unlikely due to the centralised enforcement of the DMA which allows the Commission to avoid the definition of the market, the dominant position, and the effects of the abusive conduct, which makes the enforcement of DMA remedies easier.[153] On the other hand, if the ex-post enforcement is brought by the National Competition Authority against the same undertaking or gatekeeper on the same fact to impose further obligations, it will be necessary to assess whether the exemption provided

[142] *Slovak Telekom* (n 21).
[143] Case C-117/20, *bpost SA v Autorité belge de la concurrence* [2022].
[144] Case C-151/20, *Bundeswettbewerbsbehörde v Nordzucker AG and Others* [2022].
[145] Charter of Fundamental Rights of the European Union, Article 52, (n 140).
[146] Dimitrios Katsifis, '*Ne bis in idem* and the DMA: the CJEU's judgments in bpost and Nordzucker' [2022] <https://theplatformlaw.blog/2022/03/28/ne-bis-in-idem-and-the-dma-the-cjeus-judgments-in-bpost-and-nordzucker-part-i/>.
[147] Digital Markets Act, Recital 10.
[148] Wernhard Möschel, 'The Proper Scope of Government Viewed from an Ordoliberal Perspective: The Example of Competition Policy' (2001) 157(1) Journal of Institutional and Theoretical Economics (JITE) / Zeitschrift Für Die Gesamte Staatswissenschaft.
[149] Margrethe Vestager, 'Competition for a fairer society' Speech at 10th Annual Global Antitrust Enforcement Symposium, Georgetown (20 September 2016). On the social goals of the EU Competition Law see also Ariel Ezrachi, 'Sponge' (2016) 5(1) Journal of Antitrust Enforcement 49.
[150] Article 114, Consolidated Version of the Treaty on the Functioning of the European Union [2008] *OJ C 326*.
[151] Huishsin Kuo, 'Competition in EU Digital Markets' (2022), Faculty of Law Lund University Student Papers.
[152] Katsifis (n 146).
[153] Monti (n 102).

by Article 52(1) of the Charter can be applied. The analysis, based on *bPost*,[154] will concern the definition of legal interests protected by the two legal tools. Nevertheless, scholars have highlighted that the DMA is an instrument of Competition Law, implementing the shift from a more economic approach to a more regulatory approach,[155] since it pursues the same aims as EU Competition Law.[156] Moreover, as discussed above, DMA obligations merely correspond to the recent antitrust investigations over digital platforms, increasing the difficulties in delineating the difference between DMA and EU Competition Law goals.[157]

However, in this heated debate it will be up to the Court of Justice to establish whether the DMA and the possible application of the Essential Facilities Doctrine, or Competition Law in general, pursue the same goals of keeping digital markets fair and contestable.

5 Conclusions

The acknowledgment of the competitive advantage owned by dominant platforms led the European Union Legislator, in particular the European Commission, to take action in order to protect competition on the merits and sanction situations of abuse of a dominant position.[158] In this context, a revitalisation of the historical Essential Facilities Doctrine has been claimed by several scholars who recognised that the ownership of e-commerce platforms, app stores, search engines, data, and interoperability information enable a dominant undertaking to leverage its market power in the downstream markets.[159] However, the application of the doctrine under the refusal to deal theory of harm represents a limit, more than the criteria developed by the Court of Justice, to its effectiveness. In fact, not only a specific refusal to supply competitors with an indispensable asset can lead to elimination of actual and potential competition. Even unfair conditions of treatment in the platform can lead to the same situations where toxic competition, indicated by Stucke and Ezrachi, will always create the same winner.[160] Furthermore, the acknowledgment of the essentiality of platforms is encompassed in the new ex-ante sector regulation, the *Digital Markets Act*, which will start applying in 2023. Similarities between the Essential Facilities Doctrine and the DMA, adopted under the Article 114 TFEU as a tool to avoid fragmentation in the internal market, are several, but there is doubt about their complementarity. Firstly, the definition of gatekeepers and their core platform services fulfils the first three conditions of the doctrine, notably, the

[154] *bpost SA* (n 143).
[155] Marco Cappai and Giuseppe Colangelo, 'Taming digital gatekeepers: the more regulatory approach to antitrust law' (2021) 41 Computer Law & Security Review 105559 (online).
[156] Schweitzer (n 108).
[157] Giuseppe Colangelo and Marco Cappai, 'A Unified Test for the European Ne Bis in Idem Principle: The Case Study of Digital Markets Regulation' (2021) <https://ssrn.com/abstract=3951088> accessed 29 March 2023.
[158] Article 102, *Consolidated Version of the Treaty on the Functioning of the European Union* 2008 *OJ C 326*.
[159] Guggenberger and Nikolas (n 60).
[160] Maurice E Stucke and Ariel Ezrachi, *Competition Overdose* (Harper Business 2020).

indispensability of core platform services, the elimination of competition in the downstream market, and the need to stimulate innovation around the platform. Moreover, the DMA aims at preventing all exploitation of consumers, manifesting the typical ordo-liberal influence in European Union Law. The obligations set out in the sector regulation reflect the obligations that can be imposed under the EFD ex-post enforcement, nowadays without necessity to prove the indispensability. Furthermore, they recall the most recent case law and investigations on Google, Amazon, Facebook, Apple, and Microsoft, both at National and European level. The problems with the *ne bis in idem* principle are not easy to overcome; in fact, a possible reversion to an "*idem crime*" approach in the Competition Law field cannot be set aside, since the DMA might be interpreted as no more than an implementation of Article 102 TFEU. Anyway, further research into the lively debate on the goals of EU Competition Law and its interrelation with the DMA is necessary, while waiting for the Court of Justice to take a position on these matters.

Gregory Chan*

ANTI-MONEY LAUNDERING LAWS: A THORN IN THE SIDE OF THE FOUR ASIAN TIGERS

Abstract

The Four Asian Tigers are often characterised by their surge of economic growth, and have come to represent rapid industrialisation albeit with a dash of authoritarianism. Indeed, the economies of Hong Kong, Singapore, South Korea and Chinese Taipei had undergone an unprecedented level of development in an extremely short span of time following decolonialisation, causing the World Bank to dub them "The East Asian Miracle". Yet, as the world moves into the digital age, new hurdles present themselves on the horizon for these mammoths to overcome. Of these, one of the tallest, and perhaps most unpredictable, seems to be the increasingly disruptive nature of decentralised digital assets ("DDA"). Since the launch of Bitcoin in 2008, the use, development and activity of DDAs has been growing at an unprecedented rate across the globe. With a global market cap of over $1 Trillion USD in crypto-assets alone, DDAs undoubtedly would play a significant role in the modern global economy.

Yet, despite the huge potential around these assets, policy-makers have become particularly wary of these DDAs. The emphasis on their decentralised nature has presented them as a way for users to undermine the traditional regulatory mechanisms. Particularly here, DDAs have gained notoriety as tools for assisting in money-laundering, and bypassing state-imposed economic sanctions. Studies by the International Federation of Accountants here note 5 common ways these occurs: (1) predicating crime, (2) converting illegally obtained digital assets into tangible assets, (3) hiding transactions through anonymised services, (4) layering numerous exchanges of assets from tangible to intangible to mask transactions, and (5) the integration and legitimisation of income. In light of these concerns, regional harmonised approaches seem to be taking centre stage. In Europe, significant discussion has been placed around the recent Markets in Crypto-Assets Regulation. On the other side of the Atlantic, the United States seems to be working on similar provisions, following the recent leak of the draft bill regulating DeFi and Decentralised Autonomous Organisations ('DAO"). Yet, such a harmonised approach seems to be lacking in Asia. Instead, competition between the Asian Tigers to attract investors has resulted in starkly individualised approaches among them, each looking to out-position the other to take advantage of these new developments. However, this disharmonised and fragmented approach ultimately led to cracks appearing in the regulatory firewall, often through policy oversights.

This paper will thus take a comparative, and law-economics based approach towards the law governing DDAs across these 4 high-income economies, particularly the laws governing transnational anti-money laundering mechanisms, and the place of DDAs in the law of sanctions among these nations. It primarily considers this from the perspectives of DDAs as a tool, and their impacts on how nation-states craft anti-money laundering laws ("AML"). While it ultimately concludes that the fragmented approach is acceptable given the current

* King's College London, LLB. gregory.chan@kcl.ac.uk. All information contained in this paper represents the view and opinion of the author, and does not necessarily represent the views of the publishers or affiliated organisations. Any errors are solely the fault of the authors.

situation, greater cooperation between both private and public stakeholders is imperative towards the development of the law of sanctions.
In doing a comparative analysis within these economies, this paper looks at 2 key areas within AML on digital assets. Firstly, it considers the extent of which regulatory mechanisms (such as disclosure of identities) interact with these DDAs within the local economies. Then, it considers how sanctions target DDAs, and the relevant AML laws. A further dimension that is also explored is the role of Virtual Asset Service Providers ("VASPs") within these economies, and the nature of the set of rights which are attached to these DDAs. It then discusses how this domestic legislation would interact with the growing body of international law instruments that have been in the works, including the guidelines introduced by the Financial Action Task Force ("FATF"), and the United Nations International Institute for the Unification of Private Law. It is then argued here that the crux of the interaction between the law of sanctions and domestic legislation on DDAs lies in the conversion between DDAs and tangible assets. The role of AMLs should then look to combat the conversion of "dirty" assets as a whole.
Ultimately, the comparative analysis concludes with a brief discussion of mechanisms to strengthen and, to an extent, harmonise international laws in this field. Firstly, the doctrine of comity between nations should once more be reaffirmed and strengthened. This ensures mutual recognition of regulatory attempts between these economies mutually strengthening AML legislation through the Courts in a bottom-up, but also a top-down regulatory perspective. This similarly extends to provisions around regional cooperation across the private sector, and mechanisms where these economies can implement to encourage such cooperation. Secondly, a discussion is had about the use of corporate standards for future regulatory work; concerns that AML might be too reactive, or "out-of-date" is rather prominent. Hence, futureproofing through working with various stakeholders to develop comprehensive frameworks to encapsulate the relevant features and novelties with DDAs would prove invaluable. Such would then allow these economies to fully utilise DDAs to their full potential while ensuring compliance with the law of sanctions.

JEL CLASSIFICATION: F39, F50, G28, K29, P10, P59

SUMMARY

1 Introduction

In recent years, Decentralised Digital Assets ("DDAs") has become the talk of the town. The advent of cryptocurrencies stemming from the now infamous Bitcoin Manifesto[1] has spiralled into over countless new currencies built on unique variants of blockchain technologies.[2] In the public sector, central banks have begun bilateral and multilateral discussions and initiatives to venture into the world of Financial Technology ("FinTech") and DDAs, embracing these technological developments in various ways.[3] Indeed, DDAs have undoubtedly caused significant disruptions within the global financial market in a myriad of ways. However, as with new developments, growing concerns have been raised over their use. Given the anonymity and transboundary nature of the internet, coupled with the decentralised and deregulated nature of DDAs, one can definitely understand the fears policy-makers have over DDAs. This is made worse especially with the current peer-to-peer model of DDAs which seems to bypass the paper-trail of transactions policy-makers are attempting to preserve.

As such, it seems self-evident why DDAs are particularly difficult to stomach in the law of economic sanctions. Traditionally, economic sanctions are used as a punitive measure against State's wrongful conduct. In practice however, the imposition of economic sanctions is rare, usually extremely targeted and only used in serious and extreme cases. Most recently, the 2022 invasion of Ukraine prompted a series of sanctions against Russia and Belarus, designed to narrowly target those in the upper ranks of the Russian government.[4] Similarly, in sanctions imposed against Argentina during the Falklands War, general trade sanctions were limited; instead, the targeted sanctions on the arms supply aimed to mitigate the conflict on the ground when it was deemed that the conflict would be resolved through gunfire.[5] Even when sanctions are enacted through United Nations Security Council ("UNSC") resolutions, they are generally designated against key figures,[6]

---

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 1,6. <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> accessed 5 December 2022.

[2] Xian Rong Zheng and Yang Lu, 'Blockchain Technology - Recent Research and Future Trends' (2021) 16(12) Enterprise Information Systems, <https://www.tandfonline.com/doi/full/10.1080/17517575.2021.1939895> accessed 3 December 2022.

[3] For instance, see here regarding Project BENJA, a partnership between Deutsche Bank, Hashstacs Pte Ltd, Bursa Malaysia, the UBS Group AG, the Union Bank of Philippines, and the Monetary Authority of Singapore: <https://stacs.io/wp-content/uploads/2021/05/Project-Benja-Public-2021.pdf> accessed 21 March 2023. There are similar projects in the field such as Project Genesis by the government of Hong Kong and the BIS Innovation Hub: <https://www.bis.org/publ/othp58.htm> accessed 1 December 2022.

[4] Ruth Endam Mbah and Divine Forcha Wasum, 'Russian-Ukraine 2022 War: A Review of the Economic Impact of Russian-Ukraine Crisis on the USA, UK, Canada, and Europe' (2022) 9(3) Advances in Social Sciences Research Journal 144.

[5] N Piers Ludlow, 'Solidarity, Sanctions and Misunderstanding: The European Dimension of the Falklands Crisis' (2021) 43(3) The International History Review 508 <https://doi.org/10.1080/07075332.2020.1791226> accessed 2 December 2022.

[6] Gary C Hufbauer and Barbara Oegg, 'Targeted Sanctions: A Policy Alternative' (2000) 32(1) Law and Policy in International Business 11.

or limiting a State's means to continue wrongful conduct.[7] In that regard, while sanctions seek to punish, States largely use them to target those involved and directly responsible for the State's actions rather than the general populace.

Of course, there have been sanctions imposed which are aimed at the wider populace in an attempt to incite societal pressure against the ruling government. Notable examples of this include overall trade sanctions made against the Democratic People's Republic of Korea ("DPRK") since its first nuclear launch program in 2006,[8] which covered general travel and trade, as well as the sanctions against Iran for its Nuclear Program.[9] While the DPRK's situation is unique, with a more tightly controlled government masking the effects of the sanctions to the general populace, the sanctions in Iran tell a different story. The Iranian sanctions caused a weaker currency, resulting in individuals suffering a higher cost of living as the price of exports increased.[10] Further, many oil and gas multinational corporations operating in Iran were forced to leave the country despite them being major players within the Iranian economy.[11] This exodus cost significant job shortages and many had no livelihoods amidst the inflation occurring in the country.[12] While the actual effect of these sanctions remains arguable in pushing Iran to signing the Joint Comprehensive Plan of Action,[13] they nonetheless showcase the societal impact of sanctions on a State's populace.

The imposition of these sanctions is, at its core, a top-down approach by the State. Within the State imposing sanctions, domestic laws are drafted to prevent corporations and individuals from engaging with trade with a particular State. Often, a breach of sanctions carries criminal liability within the sanctioning State's jurisdictions.[14] The United States has even gone so far as to call upon international law enforcement for assistance in prosecuting a foreign national accused of breaching sanctions within their

[7] Tom Ruys, 'Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework' in Larissa van den Herik (ed), *Research Handbook on UN Sanctions and International Law* (Edward Elgar Publishing 2016) 5. <

[8] John Crook, 'North Korea Rejects Past Nuclear Commitments, Tests Another Nuclear Weapon, and Provokes Additional UN Sanctions.' (2009) 103(3) American Journal of International Law 597.

[9] Mehdi Khalaji, 'Great Expectations: Iran after the Deal' (2015) 38(3) The Washington Quarterly, 61 <https://www.tandfonline.com/doi/abs/10.1080/0163660X.2015.1099025> accessed 2 December 2022.

[10] Ali Feghe Majidi and Zahra Zarouni, 'The Impact of Sanctions on the Economy of Iran' (2020) 8(4) International Journal of Resistive Economics, 49 <http://www.oajre.ir/article_125414.html> accessed 2 December 2022.

[11] Nikolay Kozhanov, 'U.S Economic Sanctions Against Iran: Undermined by External Factors' (2011) 18(3) Middle East Policy 144.

[12] Orkideh Gharehgozli, 'An estimation of the economic cost of recent sanctions on Iran using the synthetic control method' (2017) 157 Economic Letters 141 <https://www.sciencedirect.com/science/article/abs/pii/S0165176517302331> accessed 3 December 2022.

[13] For a discussion of sanctions following a joint comprehensive plan of action, see Farhad Rohan and others, 'The Impact of Implementing Sanction by the Party of the Six Countries (5+1) in the Joint Comprehensive Plan of Action in Exercising the International Upstream Oil Agreements from the Point of the View of Iran's Legal System' (2021) 13(24) Civil Jurisprudence Doctrines 163.

[14] See, for example, in South Korea, Art 27(1)-(8) of the Foreign Exchange Translation Act imposes criminal liability for breach of sanctions. More broadly, discussed in Nicolas Angelet, 'Criminal Liability for the Violation of United Nations Economic Sanctions' (1999) 7(2) European Journal of Criminal Law and Criminal Justice 89.

jurisdictions.[15] Of course, the enforcement of sanctions is significantly easier when trade is conducted through tangible goods and with legal tender. Tracking the paper (or electronic) trail of the movement of money has never been easier. Anti-money laundering ("AML") mechanisms adopting modern technological innovations have been increasingly applied to tackle breaches of sanctions.[16] For instance, embracing machine for transaction monitoring learning to identify suspicious patterns has strengthened AML laws globally.[17] These developments are undoubtedly to be applauded, as States seem to be moving with the rapid development of technological trends through the years.

As a whole, sanctions can only be enforced if there is sufficient oversight to monitor ongoing transactions. Conversely however, DDAs have been designed to avoid third party oversight within transactions with its peer-to-peer model. While one might consider this to be the role of DDA custodians, there is similarly difficulty with this position. These custodians, more commonly known as 'wallets', and operate as a platform for individuals to interact with their DDAs, as well as transfer DDAs to and from other users.[18] However, due to the sheer number of custodians, the inability of them to track transactions, as well as terms regarding the ownership of these assets, these custodians cannot be regarded as central institutions. The same can be said for exchanges, servers, nodes, as well as other 'custodial' platforms.[19] Instead, these should be regarded as services which other holders of these assets provide. While ownership of the DDA remains with the true owner, the DDA custodian acts as a platform to utilise these assets as though they were tangible. With so many different custodians, it further undermines any attempt at creating a regulatory environment. As a result, certain countries have been reported to have used DDAs to commit "cybercrimes", utilising these DDAs as a mechanism to avoid sanctions which were imposed on them.[20] Such practical considerations undoubtedly exemplify the importance of this discussion.

Despite these hardships, four strong economies which have a history of embracing and taking advantage of technological developments are taking this challenge head on. Characterised by the surge of rapid economic growth in wake of attaining independence,

[15] AFP, 'Singaporean wanted by US over North Korea is in Singapore: Police' *Alarabiya News* (Singapore, 6 November 2022) <https://english.alarabiya.net/News/world/2022/11/06/Singaporean-wanted-by-US-over-North-Korea-is-in-Singapore-Police> accessed 30 November 2022.
[16] David Cortright and George A Lopez, *Smart Santions: Targeting Economic Statecraft* (Rowman & Littlefield publishing, 2002).
[17] Gökberk Bayramoğlu, 'An Overview of the Artificial Intelligence Applications in Fintech and Regtech' (2017) 1 The Impact of Artificial Intelligence on Governance, Economics and Finance, 291 <https://link.springer.com/chapter/10.1007/978-981-33-6811-8_15> accessed 2 December 2022.
[18] Richard Walker and others, 'The unique and complex consideration of digital asset custody' (2021) 13(2) Journal of Securities Operations & Custody 2, 150.
[19] See, a discussion here in Harry Leinonen, 'Decentralised Blockchained and Centralised Real-Time Payment Ledgers: Development Trends and Basic Requirements' in Jakub Górka (ed), *Transforming Payment Systems in Europe* (Springer Link 2016).
[20] See, for instance, the case of North Korea at: DPRK Cyber Threat Advisory, 'Guidance on the North Korean Cyber Threat' (Government of the United States of America, 2019) <https://www.cisa.gov/uscert/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf> accessed 2 December 2022.

the Four Asian Tigers once more seem poised to embrace these new disruptions. Dubbed as the "East Asian Miracle" by the World Bank,[21] it would seem that these economies are once more attempting to be global leaders within the FinTech World. Indeed, one can similarly argue that Singapore, South Korea, Hong Kong, and Chinese Taipei have all been vying to be the London or New York of the East - the financial hub for the region.[22] Thus, their abilities to be able to take advantage of these new technologies would likely give them the necessary edge in the competition in this era of digitisation. Unfortunately, such competition has similarly resulted in starkly individualised approaches to be adopted between these countries, as they look to out-position the other. Unfortunately, where there is disharmony among nations despite the transboundary nature of the issues, there is a growing concern of cracks appearing in the regulatory firewall appearing in these assets.

This paper will thus take a comparative approach to the regulatory framework of DDAs across the Four Asian Tigers. In particular, it will comment on three areas within their regulatory framework - its definition of DDAs, its climate for DDA investors operating within their countries, internal Anti-Money Laundering ("AML") provisions and transboundary regulations and compliance with sanctions. Finally, it will analyse the position of each country and discuss potential areas for a harmonised framework to be adopted within this field.

As a brief disposition, Section II will discuss and comment on the laws found within each of the Four Asian Tigers in two areas – the general regulatory framework of DDAs, and how DDAs interact with AML and economic sanction legislation. Section III then takes a comparative view and discusses the position of these economies in three sub-sections – their taxonomies, treatments of DDAs, and compliance with existing international frameworks. Section IV discusses potential reforms that can be taken in moving towards a harmonised approach. Section IV concludes.

2 An overview of DDAs across the Four Asian Tigers: a comparative approach

As briefly alluded to earlier, DDAs have been treated significantly differently across the jurisdictions of the Four Asian Tigers. While it can be said that all these economies have a seemingly pro-DDA attitude, it is worth exploring them in greater detail to understand the nuances behind their policy-making. In that regard, this section seeks to provide an overview of the regulatory framework around DDAs.

[21] Nancy Birdsall and others, 'The East Asian miracle : economic growth and public policy : Main report (English)' (26 September 1993, World Bank Reports) <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/975081468244550798/main-report> accessed 4 December 2022.
[22] Darryl S L Jarvis, 'Race for the money: international financial centres in Asia' (2011) 14 Journal of International Relations and Development, 60.

To that end, there are three key themes which it will follow through its analysis. First, the jurisdiction's taxonomy surrounding digital assets. Second, internal domestic AML provisions and mechanisms surrounding DDAs. Finally, transboundary frameworks and compliance with international obligations. It is ultimately hoped that these three key areas will provide a holistic overview of DDAs and the law of sanctions in these jurisdictions.

2.1 Singapore

2.1.1 The regulatory framework of DDAs in Singapore

Beginning first with the small island State of Singapore. Singapore is not unfamiliar with embracing technological developments as a means to boost its economy. Since gaining independence 1965,[23] the government has been seeking to take advantage of the "latest trends" in the market. Beginning with the Civil Service Computerisation Program in the 1980 which saw the first adoption of information and communication technologies,[24] Singapore continuously adapted to the technological developments with initiatives such as SingPass[25], the Smart City project.[26] Most recently, Singapore launched GovTech - a government branch dedicated to leading digital transformation in the country.[27] Given this, it seems clear that the government is dedicated to embracing technological change, rather than shunning them away.

This trend has similarly carried over to the realm of DDAs. With Singapore touting itself as the "FinTech Hub of Asia", the country has been particularly receptive to DDAs. The Monetary Authority of Singapore ("MAS") has been extremely active in discussing technological trends in the financial world. Adopting a wide definition of DDAs, s.2 of the Payment Service Act 2019 ("PSA") hence defines them under the umbrella term "digital payment tokens", which are expressly mentioned to include cryptocurrencies.[28] In particular, the PSA writes that:

[23] Reuben Ng, Paul Wong and Si Qi Lim, 'Singapore: 50 Years of Science and Technology' (8 August 2018, Global-is-asian, Lee Kuan Yew School of Public Policy) <https://lkyspp.nus.edu.sg/gia/article/singapore-50-years-of-science-and-technology> accessed 21 March 2023.
[24] Kwok Cheong Lee, 'Civil Service Computerisation - the Singapore experience' (Expert Group Meeting on Integrating Information Systems Technology in Local Regional Development Planning, 31 October 1988). <https://dr.ntu.edu.sg/bitstream/10220/485/1/AMIC_1988_OCTNOV(VOL_1)_11.pdf> accessed 3 December 2022.
[25] Jezon Ow, 'The future of healthcare in Singapore. How an integrated use of A.I., Internet-of-Medical things (IoMT), Blockchain-based technologies, and Cloud-computing-based Medtech and Digital Health solutions will radically address medical data integrity concerns' (1 November 2021). <https://ssrn.com/abstract=3965116> accessed 3 December 2022.
[26] Ahm Shamsuzzoha and others, 'Smart city for sustainable environment: A comparison of participatory strategies from Helsinki, Singapore and London' (2021) 114 Cities.
[27] Woo Jun Jie, 'Technology and governance in Singapore's smart nation initiative' (HUP 2018).
[28] Monetary Authority of Singapore, 'Digital Payment Tokens' (November 2021, Government of the Republic of Singapore) <https://www.mas.gov.sg/-/media/MAS-Media-Library/who-we-are/mas-gallery/MAS-Gallery/Digital-Payment-Tokens.pdf> accessed 5 December 2022.

> "digital payment token" means any digital representation of value (other than an excluded digital representation of value) that
> (a) is expressed as a unit;
> (b) is not denominated in any currency, and is not pegged by its issuer to any currency;
> (c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;
> (d) can be transferred, stored or traded electronically; and
> (e) satisfies such other characteristics as the Authority may prescribe.

The PSA similarly distinguishes digital payment tokens from the concept of "e-money" through the "official currency" requirement in the Act.[29] This is particularly welcome amidst the pseudo "peer-to-peer" instantaneous bank transfer technology such as PayLah and PayNow which is particularly prevalent in the small island State.[30] For digital custodians and intermediaries, s.6 of the PSA requires digital payment token service providers to obtain a licence from MAS prior to operation. These licences carry further obligations for service under the PSA. These include the obligation of licensee to notify the authorities of certain events (s.15 PSA), obligation of licensee to provide information to Authority (s.16 PSA) and the obligation of licensee to submit periodic reports (s.17 PSA). Further, under the recent Financial Services and Markets Act 2022, the MAS has the authority to conduct inspections on these service providers to ensure compliance with these provisions. Hence, despite the nature of DDAs being fundamentally decentralised, the Singaporean Government seems to be attempting to claw power back from these custodial platforms back to the central authorities.

Despite the attempts of such a wide umbrella term, it must be noted that "digital payment token" under the PSA excludes digital securities, distinguishing them from the realm of these tokenised assets.[31] These digital securities are instead regulated under the Securities and Future Act 2001 ("SFA"); the criteria laid out under the s.2 of the SFA provide an exhaustive list to determine whether a DDA is a token under the FSA, or a tokenised security under the SFA. Such similarly reflects the ongoing policies of the MAS to be pro-DDA, but hostile towards cryptocurrencies and forms of digital property.[32]

[29] S.2, Singapore Payment Service Act 2019 <https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220> accessed 21 March 2023.
[30] See the statistics provided in: Statista, 'Singapore: Leading e-payment services by age 2022' (December 2022). <https://www.statista.com/statistics/1106658/singapore-leading-e-payment-services-by-age/> accessed 7 December 2022.
[31] Monetary Authority of Singapore, 'A Guide to Digital Offering', (26 May 2020, Government of the Republic of Singapore) paras. 1.2, 2.1 <https://www.mas.gov.sg/-/media/MAS/Sectors/Guidance/Guide-to-Digital-Token-Offerings-26-May-2020.pdf> accessed 30 November 2022
[32] Monetary Authority of Singapore, 'Yes to Digital Asset Innovation, No to Cryptocurrency Speculation' - Opening Address by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Green Shoots Seminar on 29 August 2022, (29 August 2022, Government of the Republic of Singapore) <https://www.mas.gov.sg/news/speeches/2022/yes-to-digital-asset-innovation-no-to-cryptocurrency-speculation> accessed 29 November 2022.

Indeed, it seems that MAS is looking to adopt a "wait-and-see" approach before making a clear distinction in these assets; to "look beyond labels and examine features and characteristics of each token".[33]

From a practical perspective, this distinction might explain the decisions of the Courts to allow proprietary injunctions of non-fungible tokens where they were regarded as securities rather than a form of payment tokens.[34] The position however, is currently unsettled for cryptocurrencies, where the Apex Court in *Quoine Pte Ltd v B2C2*[35] declined to comment on whether "[bitcoin], may even be regarded as a species of property capable of attracting trust obligations." despite citing the United Kingdom's Jurisdiction Taskforce's analysis on crypto-assets[36] which concluded that crypto-assets could be treated as having a proprietary character.[37] Nonetheless, as cryptocurrencies were suggested to form part of the legislation of digital securities or a 'security-based derivative contract',[38] it is likely that they would be caught under this Act, and cement its proprietary character.

A final category that must be discussed is 'stablecoins', given its unique position in Singapore's regulatory environment. While traditional cryptocurrencies such as Bitcoin and Ethereum are predominantly floating and speculative, stablecoins are described as a fiat currency, backed by a different form of asset.[39] In the private sector, the most common crypto-assets known as stablecoins are Tether Gold (Ticker: XAUT) and Paxos Gold (Ticker: PAXG) are backed with gold.[40] The MAS seems to have special considerations for these coins, and is even looking to promote them despite their hostile approach towards traditional cryptocurrencies.[41] However, an analysis of the proposed changes indicates that these requirements once more suffer from attempts to 'centralise' these

[33] (n 30). See also: Monetary Authority of Singapore, *Money at a Crossroads: Public or Private Digital Money?* - Summary of Panel Remarks by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at IMF Seminar on Money at a Crossroads on 18 April 2022" (18 April 2022) <https://www.mas.gov.sg/news/speeches/2022/money-at-a-crossroads-public-or-private-digital-money> accessed 2 December 2022.
[34] *CLM v CLN* [2022] SGHC 46. However, the term "digital securities" was not mentioned through the decision, nor was the Securities and Futures Act 2001. However, the reasoning from the judgement is similar to the distinction made between DPTs and securities.
[35] *Quoine Pte Ltd v B2C2* [2020] SGCA(I) 02.
[36] ibid para 57 and para 143.
[37] UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019) The LawTech Delivery Panel 21, 22 [85] <https://resources.lawtechuk.io/files/4.%20Cryptoasset%20and%20Smart%20Contract%20Statement.pdf> accessed 1 December 2022.
[38] Kenneth Pereire and Lin YingXin, 'KGP Legal LLC' in Joasis N Dewey (ed), *Blockchain & Cryptocurrency Laws and Regulation 2023* (Global Legal Insights 2022).
[39] Makiko Mita and others, 'What is Stablecoin? A Survey on Price Stabilization Mechanisms for Decentralised Payment Systems' 8th International Congress on Advanced and Applied Informatics (2019) 60 <https://ieeexplore.ieee.org/abstract/document/8992735> accessed 2 December 2022.
[40] Akanksha Jalan, Roman Matkovskyy and Larisa Yarovaya, '"Shiny" crypto assets: A systemic look at gold-backed cryptocurrencies during the COVID-19 pandemic' (2021) 78 International Review of Financial Analysis <https://doi.org/10.1016/j.irfa.2021.101958> accessed 7 December 2022.
[41] Monetary Authority of Singapore, *MAS proposes measures to reduce risks to consumers from cryptocurrency trading and enhance standards of stablecoin-related activities* (26 October 2022, Government of the Republic of Singapore); Monetary Authority of Singapore, *Consultation Paper: Proposed Regulatory Approach for Stablecoin Relate Activities* (Government of the Republic of Singapore, October 2022).

fundamentally 'decentralised assets'. Proposed regulations include oversight of the issuers of the currency stablecoins are pegged to, disclosure obligations, as well as background checks for users and holders of these currencies.[42] It is also worth noting that express wording that MAS to describe decentralised stablecoins is "well-regulated and securely backed."[43] In essence, such regulations would place users of stablecoins in a similar position as using traditional currencies, rather than anything unique or different. Such would consequently have stablecoins lose their unique identities within the DDA framework.

Ultimately, the position of DDAs in Singapore seems to have been flipped on its head. On one hand, the country seems to be extremely positive towards incorporating and embracing DDAs as a whole, believing it to constitute the next generation of payments. Yet, it cannot accept concepts of decentralisation and ownership of DDAs, and seeks to shelter this novel financial instrument under a regulatory climate of obligations. While this may yield benefits to ensure a less volatile, less speculative and more certain markets for greater use in international trade, such a framework unfortunately seems to undermine the whole purpose of DDAs as a peer-to-peer model. Nonetheless, for the purposes of AML and compliance with sanctions, such regulatory oversight would, at first glance, seem beneficial.

2.1.2 AML laws and economic sanctions of DDAs in Singapore

Having delved into the Nation-State's position on DDAs' one can then consider its implications on AML laws. To briefly summarise the position above, the laws governing DDAs in Singapore are split into two categories. First, digital payment tokens under the PSA, where tokens operate as a form of 'decentralised currency' exchanged on licensed online platforms complying with the relevant obligations. Examples of these digital payment tokens generally include the traditional cryptocurrencies - Bitcoin, Etherum. Second, digital securities traded under the SFA which stem from securities-based contracts on the blockchain. These include tokenised commodities, as well as modern innovations such as blockchain-based green bonds,[44] and bank-backed debt instruments,[45] to name a few. In both instances however, Singapore's MAS was similarly quick to refer to the Terrorism (Suppression of Financing) Act 2002 ("TSFA"), as well as international instruments such as UNSC within their guidance documents for their anti-AML provisions.[46] These key pieces of legislation in Singapore include the:

[42] ibid.
[43] ibid.
[44] Project Benja, *An MAS Financial Sector Technology & Innovation (FSTI) Scheme Proof-of-Concept* (2020-2021) <https://stacs.io/wp-content/uploads/2021/05/Project-Benja-Public-2021.pdf> accessed 4 December 2022.
[45] Monetary Authority of Singapore, *MAS Partners the Industry to Pilot Use Cases in Digital Assets* (31 May 2022, Government of the Republic of Singapore) <https://www.mas.gov.sg/news/media-releases/2022/mas-partners-the-industry-to-pilot-use-cases-in-digital-assets> accessed 28 November 2022.
[46] Statista (n 30), para 3.2.2.

1. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992,
2. MAS Notice PSN01 'Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services),
3. the MAS Notice PSN02 'Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service)';
4. and the MAS Notice SFA04-N02 'Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries'.[47]

For digital payment tokens, obligations under the FSA require DDA custodians registered in Singapore to conduct regular risk assessment procedures, which includes customer and beneficiary due diligence.[48] Further, MAS has similarly informed these service providers that they have obligations to report suspicious transactions under AML regulations, and comply with sanctions against terrorism activities listed under the Combating the Finance of Terrorism ("CFT") provisions.[49] Where transactions are carried out by entities under CFT provisions, the TSFA similarly requires custodians to disclose these transactions to the MAS.[50]

These AML provisions are particularly thematic, given that they are largely contingent on obligations around the provisions of the licence granted to service provided. For instance, where these licences impose rather onerous disclosure obligations on DDA custodians, their AML framework becomes contingent on the appropriate verification of the identities of persons who operate on these custodians. Such seems to suggest a stringent top-down approach for custodians operating and providing services in Singapore. Similarly, to attempt to dissuade unlicensed DDA custodians from operating, the s.4(4) of the FSM has laid out particularly onerous fines for institutions who do not comply with these provisions.

Unfortunately, a majority of the provisions surrounding digital payment tokens in Singapore are silent on their compliance with international obligations and international law instruments; the exception being express reference to UNSC resolutions.[51] Nonetheless, s.15 FSM does note that the MAS has the final say on determining the compliance of DDA custodians with the State's international law obligations under the broader header of the "public interest". The MAS has recently exercised this power

[47] Kenneth George Pereire and Lin Yingxin, 'The Virtual Currency Regulation Review: Singapore' in Paul Anderson (ed), *The Virtual Currency Regulation Review* (The Law Reviews 2022).
[48] s.16 Financial Service and Markets Act 2022. More specifically, referenced in: Monetary Authority of Singapore, "Prevention of Money Laundering and Countering the Financing of Terrorism - Banks". (24 April 2015, MAS Notice 626). <https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/notices/AMLD/notice-626/MAS-Notice-626-last-revised-on-1-March-2022-1.pdf> accessed 25 November 2022.
[49] Statista (n 30). See also: s. 45 of the *Terrorism (Suppression of Financing) Act* 2002
[50] Cf s.16(3) of the *Finance and Securities Market Act* 2022.
[51] Statista (n 30), para 3.2.2.

following the global sanctions imposed against Russia, despite the lack of a UNSC resolution imposing sanctions on Russian authorities.[52] In effect, such requires DDA custodians to restrict their client's ability to transfer assets to Russian beneficiaries.[53] As such, it is evident that Singapore's mode of handling digital payment tokens is rather traditional, and falls along the lines of how sanctions are enforced on domestic companies within the physical world.

For digital securities governed by the SFA, the situation remains significantly simpler. While the FSA itself does not make express provisions for governing the trade of decentralised securities, the Singaporean Government makes blanket umbrella bans against the trading of these assets against sanctioned countries. For instance, global sanctions imposed against Russia include a blanket ban for financial institutions to create business relationships with the relevant Russian banks. On that basis, DDA-securities traders in Singapore would be unable to tap on decentralised tokenised securities based in Russia, such as the Atomyze token.[54] However, for countries sanctioned by UNSC resolutions, Singapore's domestic legislation enforcing these provisions operates differently. Sanctions against Iran,[55] Libya,[56] Yemen,[57] among other countries, do not mention a general ban for the use of DDA-securities. Perhaps this could be explained by the different economic developments these countries enjoy - Russia having a more significantly developed digital infrastructure and hence, requiring express provisions. Similarly, some of these countries have express bans on DDAs and do not embrace tokenised securities.[58] However, closer analysis of the imposed sanctions indicate that these are narrow targeted sanctions imposed by the country on certain individuals or activities. In that regard, the lack of express prohibitions for DDAs is thus unnecessary, and would fall outside its scope.

As a whole, Singapore's regulatory climate surrounding AML and compliance with economic sanctions of DDAs can be said to be twofold. First, the restriction of the trading of security-based DDAs seems to flow from their obligations to comply with overall international sanctions. Where international sanctions are broad, compliance with them requires the overall prohibition of trading on these platforms. This position holds true for

[52] Peace and Security, 'Russia blocks Security Council action on Ukraine' *UN news* (26 February 2022) <https://news.un.org/en/story/2022/02/1112802> accessed 29 November 2022.
[53] Monetary Authority of Singapore, *Targeted Financial Sanctions: Financial Measures in relation to Russia* <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions> accessed 2 December 2022; Ministry of Foreign Affairs, 'Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine' (5 March 2022, Government of Singapore) <https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions> accessed 2 December 2022.
[54] See, for instance, Éva Réka Keresztes and others, 'Exploratory Analysis of Blockchain Platforms in Supply Chain Management' (2022) 10(9) Economies, 206.
[55] United Nations Act (Chapter 339), United Nations (Sanctions - Iran) Regulations 2019.
[56] United Nations Act (Chapter 339), United Nations (Sanctions - Libya) Regulations 2021.
[57] United Nations Act (Chapter 339), United Nations (Sanctions - Yemen) Regulations 2015.
[58] Younis A Younis, Abdulsalam Sami and Salme Naje, 'Blockchain and Cryptocurrencies in Libya: A Study', ICEMIS'21: The 7th International Conference on Engineering & MIS 2021, New York, United States, October 2021) <https://dl.acm.org/doi/abs/10.1145/3492547.3492594> accessed 2 November 2021.

digital payment tokens, where blanket statements and regulations have been imposed on these DDAs custodians. Conversely, the lack of guidance found within domestic AML legislation indicates that the country is largely reliant on digital custodians conducting their independent due diligence in accordance with regulations, and only intervening in extreme cases. Such similarly follows the "wait-and-see" trend which the MAS has been practising on the distinctions between digital securities and payment tokens. After all, it cannot be denied that these sanctions are often only imposed in extreme and rare cases. Hence, such an approach may allow more flexibility for the MAS to provide appropriate guidance where necessary and at a short-term notice, but also give DDA custodians means for their own discretion. While concerns might arise pertaining to legal certainty, the MAS' current approach seems to indicate that the small nation State is attempting to best embrace this novel technology, albeit through centralising the ongoing decentralisation efforts

2.2 South Korea

2.2.1 The regulatory framework of DDAs in South Korea

Not unlike the Singaporean story, the Republic of Korea (South Korea) has a history of embracing technology at every step of its development. Although it had been regarded as one of the poorest nations in the world in the 1960s after the Korean War, the country's transformation into a high-tech economic leader in the region had prompted many to dub them "The Miracle on the Han River".[59] This development was largely attributed to then President Park Chung Hee. With the economy dominated by family-run conglomerates in the past,[60] then President Park worked with these families on a close personal level, providing them economic support in exchange for socio-political approval.[61] As a result, some of these conglomerates have now become household names, which includes technology-heavy firms Samsung, Hyundai and LG.[62] This similarly propelled South Korea's economy towards becoming one of the most respected across East Asia.

In the present day, South Korea has similarly adopted a mammoth role in DDAs. Prior to its collapse, South Korea formed the home-base for the Terra-LUNA token, which had

[59] Vincent Koen and others, 'Sustaining the Miracle on the Han River', (25 October 2021, Organization for Economic Co-operation and Development). <https://www.oecd.org/country/korea/thematic-focus/sustaining-the-miracle-on-the-han-river-103653fa/> accessed 3 December 2022.
[60] Eleanor Albert, 'South Korea's Chaebol Challenge' (4 May 2018, Council on Foreign Relations), <ahttps://www.cfr.org/backgrounder/south-koreas-chaebol-challenge> Accessed 3 December 2022.
[61] Pyŏng-guk Kim, Byung-Kook Kim and Ezra F Vogel, *The Park Chung Hee Era: The Transformation of South Korea* (Harvard University Press 2011).
[62] Terry Campbell and Phyllis Keys, 'Corporate governance in South Korea: the chaebol experience' (2002) 8(4) Journal of Corporate Finance 373 <https://doi.org/10.1016/S0929-1199(01)00049-9> Accessed 4 December 2022.

a market value of over USD $20 billion.[63] Similarly, recent initiatives by the legislature include the South Korea's Act on Reporting and Using Specified Financial Transaction information 2021 ("RSFTI") showcase its willingness to adapt in the financial sphere. The RSFTI currently forms the backbone of the legislature around DDAs in South Korea and provides the Taxonomy which the Republic uses in its subsequent legislation. The RSFTI is similarly seeking to pave the way for the upcoming Digital Assets Basic Act 2023 ("DABA") which will be the leading statutory instrument for the regulation of digital assets in South Korea.

While DABA remains the long-term plan, it is nonetheless worth looking at the framework which the RSFTI has set out for DDAs. Under the RSFTI, South Korea's taxonomy on DDAs designated the term "digital assets" as the umbrella term for all intangible assets. These include e-currencies, Central-Backed Digital Currencies ("CBDCs"), as well as Decentralised Autonomous Organisations ("DAOs"). Under these "digital assets", there is a further subset which has been dubbed "virtual assets". These virtual assets are where cryptocurrencies and NFTs are governed.[64] For Korea, such a distinction seems particularly important due to their use of "critical digital assets" within national security infrastructure.[65] Hence, for the remainder of the paper, the phrase DDAs when used in the context of South Korea's regulatory framework will refer to its use of "virtual assets". For further reference, the definition of "virtual assets" was particularly broad under the RSFTI, and reads as follows:

> "electronic certificates of economic value (with the exception of electronic currency, etc. as defined under the Electronic Financial Transactions Act) that can be traded or transferred electronically."[66]

However, what is particularly interesting within the DDA framework is that "virtual assets" seems to only cover NFTs and cryptocurrencies. While these are the most common forms of DDAs, modern DDAs can encompass a significantly wider range of assets. These include decentralised tokenised securities such as green bonds or commodities, distributed ledger technologies, non-convertible intangible assets, among other matters.[67] At first glance, it would seem that these assets would, by default, fall under the wide term of "virtual assets" under the RSFTI. However, they are instead covered by the Financial Investment Services and Capital Market Act ("FISCM"), which provides its own

[63] Riccardo De Blasis and others, 'Intelligent Design: Stablecoins (In)stability and Collateral During Market Turbulence' (30 June 2022). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217910> accessed 4 December 2022.
[64] Meejeong Hwanga, Kookheui Kwonb, 'Development of an Identification Method for Vital Digital Assets Selection on Nuclear Cyber Security'' (Transactions of the Korean Nuclear Society Spring Meeting, Jeju Island, Korea, 17-18 May 2018), 3 <https://www.kns.org/files/pre_paper/39/18S-134황미정.pdf> accessed 2 December 2022.
[65] Junyoung Son, Jonggyun Choi and Hyunsoo Yoon, 'New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants' (2019) 7 IEEE Access, 78379-78390
[66] s.3(3) Act on Reporting and Using Specified Financial Transaction information 2021.
[67] Andria van der Merwe, 'A Taxonomy of Cryptocurrencies and Other Digital Assets' (2021) 41(1) Review of Business 30.

sets of regulations to securities. As such, it becomes self-explanatory why commentators are concerned about the potential conflicting legislation would create unpredictability and legal uncertainty within the digital asset market within South Korea.[68] Nonetheless, if one were to look at the current President of South Korea, Suk-Yeol Yoon's election mandate which includes the regulation of DDAs, it would seem that "virtual assets" would exclude security tokens.[69] Hence, it is likely that security tokens within South Korean legislation would fall under the FISCM, and governed by the relevant securities legislation found within the State.

While South Korea's DDA framework remains significantly younger than Singapore's current approach, it nonetheless remains important to understand how these different tokens are governed within Korea, both for users and custodians. For DDA custodians, South Korea has adopted a similar position to Singapore, requiring mandatory registration of all virtual asset service providers ("VASP") under the Korean Financial Intelligence Unit. Upon registration, they will be granted a licence to operate within the Republic.[70] Unlike Singapore however, there seems to be less of a regulatory framework surrounding VASPs, with its core obligations merely to verify customer identity, report on suspicious transactions, and follow anti-money laundering guidelines.[71]

Perhaps most crucially for VASPs, the registration process requires compliance with the Korea Information Security Management System ("K-ISMS") under the Act on Promotion of Information and Communications Network Utilisation and Information Protections (as amended in 2008). The K-ISMS is a certification based on the industry standard ISO 27001:2002, managed by the Korea Internet and Security Agency that is meant to ensure adequate protection of personal data. The K-ISMS regulations further requires users to register their personal details on VASP sites, using a real-name verifiable account. Using this, the State can then act to ensure the sites' ability to protect the data from cyber-threats through this top-down system. Consequently, while adhering to K-ISMS then removes the layer of anonymity surrounding VASPs, it nonetheless provides an additional layer of protection for peer-to-peer transactions. However, it must be emphasised that adherence to the K-ISMS framework is not unique to cryptocurrency exchanges. Almost all

[68] Han-Jin Lee, Sung Yun Kang and Mooni Kim, 'Opening the floor for global discussions: regulatory transition around digital assets in South Korea' (International Financial Law Review, 30 September 2022) <https://www.iflr.com/article/2aowsnrfgsb8r3avrw075/sponsored/opening-the-floor-for-global-discussions-regulatory-transition-around-digital-assets-in-south-korea> accessed 2 December 2022.
[69] Ik-Hwan Cho, Young Man Huh and Bumkyu Sung, 'New Administration's National Agenda on Financial Services Sector' (11 May 2021, Kim & Chang) <https://www.kimchang.com/cn/insights/detail.kc?sch_section=4&idx=24980> accessed 1 December 2022.
[70] Keundug Park and Heung-Youl Yoom, 'Proposal for Customer Identification Service Model Based on Distributed Ledger Technology to Transfer Virtual Assets' (2021) 5(3) Big Data Cognitive Computing 31 <https://doi.org/10.3390/bdcc5030031> accessed 1 December 2022.
[71] ibid.

sites which stores personal data, such as Amazon,[72] Google,[73] and Microsoft[74] all require K-ISMS compliance. Hence, such regulations form the core minimum operating requirements in Korea.

This is undoubtedly a stark departure from the full disclosure and reporting obligations which Singapore and the MAS imposes on digital payment token providers. Nonetheless, South Korea seems to wish to tap upon the "decentralised" nature of these technologies as much as possible; hence, imposing minimum obligations as opposed to a full regulatory regime. Interestingly, it seems that the overall notion of decentralisation is, in Korean culture, linked to the popular view on democracy. The 'more' decentralised something is, the more democratic the people believe it to be.[75] As such, the country's rather lax stance towards managing DDAs seems like a natural conclusion.

2.2.2 AML laws and economic sanctions of DDAs in South Korea

Despite the minimal regulatory interference which South Korea has on virtual assets providers, the emphasis on AML and compliance with sanctions remains a core pillar within South Korea's regulatory framework. Undoubtedly, attempts to preserve the decentralised nature of these assets despite them being designed to undermine these policies, and still finding a balance for strong AML policies, and sanction-compliant framework is to be applauded.

Beginning with VASP's obligations, the RSFTI was designed around strengthening AML provisions and international economic sanctions within the realm of virtual assets, while similarly ensuring VASP compliance with these regulations. Under the RSFTI, there are two core obligations for VASPs. Firstly, the "Travel Rule", for VASPs to record the originator and beneficiary's information in a transfer of DDAs.[76] Secondly, the "segregation rule", requiring VASPs should isolate these recorded transactions where they are suspicious in nature.[77] These rules operate in tandem and seek to ensure a degree of anonymity within these transactions, but also ensuring no foul play is amidst.

Beginning first with the Travel Rule, this essentially requires VASPs to record transactions about the virtual asset transfer, providing the virtual asset originator's

[72] See at: <https://aws.amazon.com/compliance/k-isms/> accessed 27 November 2022.
[73] See at: <https://cloud.google.com/security/compliance/k-isms> accessed 27 November 2022.
[74] See at: <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-korea-k-isms> accessed 27 November 2022.
[75] Jae Hyun Lee and Jaekwon Suh, 'Decentralisation and government trust in South Korea: Distinguishing local government trust from national government trust' (2021) 8(1) Asia & the Pacific Policy Studies 68 <https://doi.org/10.1002/app5.317> accessed 2 December 2022; Jong Soon Lee, 'The politics of decentralisation in Korea', (1996) 22(3) Local Government Studies 60 <https://doi.org/10.1080/03003939608433830> accessed 3 December 2022.
[76] Kibae Kim, 'Global Standards Mapping Initiative (GSMI 2.0): Standalone Paper, South Korea' (November 2021, Global Blockchain Business Council), 5.
[77] Lee & Ko, 'Amended Act on Reporting And Using Specified Financial Transaction Information Now Governs Virtaul Assets' (13 March 2020, Legal500) <https://www.legal500.com/developments/thought-leadership/amended-act-on-reporting-and-using-specified-financial-transaction-information-now-governs-virtual-assets/> accessed 3 December 2022.

information about their beneficiary as a means for information sharing.[78] This is starkly different from obligations to record and report such information to a top-down body, and leaves power in the hands of the citizens rather than the governments. Yet, it seems that the obligation is reversed for beneficiaries. If a transaction is suspicious, beneficiaries have an obligation to report these transactions to the relevant authorities under the RSFTI.[79] When these suspicious transactions are reported, VASPs then trace the relevant wallet addresses and wallet-to-wallet transactions history to match them with real-name-verification obligations under the K-ISMS framework, then allowing for surveillance units to trace the transactions of the senders.[80] Such undoubtedly exemplifies the level of trust which the Korean government has with its people. After all, respect goes both ways. Where the government seems to trust the populace, it becomes natural that the populace returns the favour.

In that regard, one thus easily identifies the importance of the "segregation rule" under the RSFTI. Following reporting obligations, it seems that the State is rather careful to ensure that only key personal information is reported; hence, segregating the suspicious activity from the remainder of the records kept by VSAP. This is similarly exemplified in the process that VASPs use to track these transactions. Despite having and requiring real-name-verification for users who sign up, VASPs only when there is a notion of suspicious activities. Hence, this protects the information of others on the platform, while allowing for a degree of regulatory oversight with minimal interference in the virtual asset marketplace.

Before delving into the interaction between virtual asset regulations and sanctions regime, it is similarly quintessential to understand South Korea's sanctions regime independently. As a State with a history of imposing sanctions on their not-too-distant neighbour - the Democratic Republic of Korea all the way back since the Korean War,[81] one undoubtedly expects this regime to be a firm one. Indeed, under the Article 5 of the Foreign Trade Act, the Minister for Trade, Industry and Economy has the discretion to impose general and specific trade embargos against nations "when it is necessary to perform duties to maintain international peace and security under treaties on trade…and generally accepted international laws and regulations".[82] An emphasis should be had on the latter words of international law, which shows respect for UNSC resolutions that impose sanctions, and similarly abiding by them when necessary. Similarly, financial sanctions can be imposed by the Minister of Strategy and Finance under the "Guidelines for payment and receipt permits for the Implementation of Obligations for the

[78] See at: <https://www.fsc.go.kr/eng/pr010101/22526> accessed 4 December 2022.
[79] National Assembly of Korea, *Act on Reporting and Using Specific Financial Transaction Information*, No 17299, Amended on 19 May 2020, Enforced on 20 May 2020.
[80] (n 75).
[81] Nazanin Zadeh-Cummings and Lauren Harris, 'The Impact of Sanctions against North Korea on Humanitarian Aid' (2020) 2(1) Journal of Humanitarian Affairs 9 <https://doi.org/10.7227/JHA.033> accessed 1 December 2022.
[82] Foreign Trade Act, Art 5(4). Also note the additional requirement of ensuring the maintenance of international law. Translated at <https://elaw.klri.re.kr/eng_service/lawView.do?hseq=37529&lang=ENG> accessed 2 December 2022.

Maintenance of International Peace and Security.".[83] Though labelled as "Guidelines", this remains an enforceable derivative legislation which imposes punitive fines when there are prohibited transactions with a term of imprisonment (maximum 3 years) or a fine (maximum KRW 200 million).[84]

Unfortunately, there seems to be a dearth in the legislation of economic sanctions and DDAs; there are no mentions of their applicability within the respective acts which governs virtual and digital assets. While Article 15(2) of the RSFTI does make a brief note about disallowing transactions that finance terrorism, as well as abiding by recommendations from international organisations with regards to virtual assets, such an approach seems too general, and not specific towards virtual assets. This top-down blanket approach by the government also does not make itself privy to the uniqueness of virtual asset technologies, such as blockchain-based transparency.[85] In that regard, an assumption can be reasonable that these sanctions would operate similar to those in Singapore, falling under the Minister of Strategy and Finance and the Financial Service Commission where these assets are treated as financial instruments.[86] Applying this to South Korea's virtual asset infrastructure, any decisions pertaining to the use of sanctions on virtual assets would likely require a harmonised approach to be taken by all VASPs, as well as the Minister for Trade, Industry and Economy to similarly enforce general trade sanctions and prevent the exchange of virtual assets for tangible goods. Hence, although decentralisation preserves characteristics, a unified approach must be adopted across these decentralised bodies.

Overall, the provisions surrounding AML regulations, and economic sanctions of virtual assets seem to be in their infancy in South Korea. Nonetheless, the strong framework which the country has set for itself has placed it on the right path towards ensuring compliance with their relevant international law obligations. Nonetheless, more work is to be had in the field of compliance with economic sanctions to ensure appropriate legal certainty within international law obligations. After all, user-trust can only go so far.

[83] Financial Action Task Force, *Mutual Evaluation Report: Anti-Money Laundering and Combating the Financing of Terrorism*, (26 June 2009, Organisation for Economic-Cooperation and Development) 49 <https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Korea.pdf> accessed 21 March 2023.

[84] *Foreign Exchange Transactions Act*, Art 27(1)-(8). Translated at <https://law.go.kr/LSW/lsInfoP.do?lsiSeq=191033&viewCls=engLsInfoR&urlMode=engLsInfoR> accessed 2 December 2022.

[85] Juan F Galvez, Juan C Mejuto and Jesus Simal-Gandara, 'Future challenges on the use of blockchain for food traceability analysis' (2018) 107 TrAC Trends in Analytical Chemistry 222.

[86] YangJay-Son, Kim Tae Yeun and Lee Tae Ho, 'Banking Regulation in South Korea: Overview'. (Thomson Reuters Practical Law, 1 November 2022) <https://uk.practicallaw.thomsonreuters.com/w-032-4691?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 3 December 2022.

2.3 Hong Kong

2.3.1. The regulatory framework of DDAs in Hong Kong

The Special Administrative Region of Hong Kong ("HKSAR") has a rather unique position in its overall governance structure. Originally a British Colony, the governance of the region was transferred to the People's Republic of China ("PRC") on the 1st of July 1997.[87] However, as part of the agreement, HKSAR was allowed to have its own economic and governance independent from mainland PRC. As a result, the HKSAR economy saw significant success as foreign investors viewed it as a pathway to expanding in Asia while China was still opening up.[88]

As a result, the influx of western influence had similarly brought an advent of technology to HKSAR, in turn, fostering a strong culture of embracing new developments to promote economic development. Even in its early days, the USD $5 Billion Innovation and Technology Fund established in 1999 by the government sought to promote the integration of technology. This fund subsequently continued and even expanded, with over USD $40 Billion injected as of July 2022.[89]

Recently, there has even been a strong push towards working with mainland PRC and facilitating mutual development between the regions. The Lok Ma Chau Loop is one example of this - currently being developed as part of the Hong Kong-Shenzhen Innovation and Technology Park initiative to further push for greater technological advancements and sharing of information between the economies.[90] As such, it should be a foregone conclusion that HKSAR is particularly receptive towards DDAs, with public private partnerships set up to explore and take advantage of these new technologies in a sustainable manner.[91]

The regulatory framework in HKSAR is led by the Financial Action Task Force, which has just passed the new Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 ("MLCTF") around DDAs, coming into force on 1 January 2023.[92] In essence, the MLCTF adopts a similar definition of DDAs to those in Korea. It uses the term "virtual assets" and defines them as an intangible representation of an asset which has economic value. More specifically, the Art 53ZRA of the MLCTF notes that a virtual asset is defined as:

[87] Joint Declaration on the question of Hong Kong. 1985.
[88] Amy Ang, 'Hong Kong: Securities Regulation after 1997 Handover' (CORE publishing, 1 January 2020) <https://core.ac.uk/download/pdf/8766482.pdf> accessed 2 December 2022.
[89] Innovation, Technology and Industry Bureau, *Hong Kong: The Facts. Innovation, Technology and Industry* (July 2022, Gov.Hk) <https://www.gov.hk/en/about/abouthk/factsheets/docs/technology.pdf> accessed 5 December 2022.
[90] See at: <https://www.hsitp.org/en/about-us/index.html> accessed 27 November 2022.
[91] Project Genesis by the government of Hong Kong and the BIS Innovation Hub: <https://www.bis.org/publ/othp58.htm> accessed 1 December 2022.
[92] Gov.Hk, *Government welcomes passage of Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022*. (7 December 2022, Gov.HK Press Release) <https://www.info.gov.hk/gia/general/202212/07/P2022120700263.htm> accessed 8 December 2022.

(1) In this Ordinance -
  (a) A cryptographically secured digital representation of value that
    (i) Is expressed as a unit of account or a store of economic value;
    (ii) Either -
      A) Is used, or is intended to be used, as a medium of exchange accepted by the public, for any one or more of the following purposes -
        I) Payment for goods or services;
        II) Discharge of a debt;
        III) Investment; or
      B) Provides rights, eligibility or access to vote on the management, administration or governance of the affairs in connection with, or to vote on any change of the terms of any arrangement applicable to, any cryptographically secured digital representation of value;
    (iii) Can be transferred, stored or traded electronically; and
    (iv) Satisfies other characteristics prescribed by the Commission under subsection (3)(a); or
  (b) A digital representation of value prescribed as a virtual asset by notice published under subsection (4)(a)
(2) A digital representation of value is excluded from the definition of *VA* in subsection (1) if -
  (a) It -
    (i) Is-
      A) Issued by a central bank, or by an entity that performs the functions of a central bank or by an entity authorised by a central bank on its behalf; or
      B) Issued by a government of a jurisdiction, or by an entity authorised by the government of a jurisdiction and acting pursuant to an authority to issue currency in that jurisdiction;
    (ii) Is a limited purpose digital token;
    (iii) Constitutes securities or a futures contract;
    (iv) Constitutes any float of SVF deposit of a stored value facility as defined by section 2 of the Payment Systems and Stored Value Facilities Ordinance (Cap. 584); or
    (v) Satisfies other characteristics prescribed by the Commission under the subsection (3)(b); or
  (b) It is a digital representation of value prescribed not to be a virtual asset by notice published under subsection (4)(b)

This is a particularly extensive definition of virtual assets under the MCLTF, which is undoubtedly to be applauded. Within it, there are clear signals that indicate HKSAR is embracing VAs. Art 53ZRA(1)(a)(A)(ii)(b) shows an understanding of on-chain governance mechanisms which have been employed recently as a mechanism for decentralised governance.[93] Further, it is also worth noting that the use of virtual assets as decentralised debt instruments, as well as investment instruments, are all found within the definition of virtual assets under Art 53ZRA(1)(a)(A)(ii)(a)(II)-(III). This is a stark difference from the positions of Singapore and South Korea where these financial instruments are governed by securities-based legislation.

Finally, it is similarly worth noting elements which are excluded from the definition of a virtual asset. Art 53ZRA(2)(a)(i) which covers CBDCs, and Art 53ZRA(2)(a)(iii) on securities and future contracts are of relevance. On the former, this is a clear recognition that these central bank digital currencies are a distinct form of virtual assets; Singapore and South Korea are currently silent on its classification. Of the latter however, a distinction seems to have been made between the use of these assets by investors (Art 53ZRA(1)(a)(A)(ii)(a)(II)-(III)), and the design of the assets by issuers. When issuers engage in the dissemination of virtual assets, such as through Initial Coin Offering, these assets would be considered to be securities and outside the scope of virtual assets.[94] Conversely, when such assets are traded by users at a later stage, they would constitute an investment under Art 53ZRA(1)(a)(A)(ii)(a)(II). Unfortunately, such a distinction seems to create some uncertainty within the current regulatory framework, particularly in the realm of the secondary markets on the applicable laws. Nonetheless, the practical reality is that service providers do not engage in the initial setting up and issuance of tokens, but rather, merely act as a custodian when these companies engage in such activities. Hence, while clarity is preferred, the current situation remains adequate given the circumstances.

Overall, HKSAR's legal framework surrounding the use of digital assets is indeed robust. Accounting for technological developments and understanding the nuances behind DDAs are efforts that should be applauded. Indeed, the distinctions made within virtual assets between its issuance and subsequent use creates a practical framework, clearly delineating the role of VASPs and private entities within HKSAR.

2.3.2 AML laws and economic sanctions of DDAs in Hong Kong

With such a broad definition of DDAs in HKSAR under the all-encompassing term "virtual assets", there would inevitably be obligations and requirements for VASPs to comply with. These licensing provisions can be found under Art 53ZRH - 53ZRS. VASPs operating within

[93] Wessel Reijers and others, 'Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies' (2021) 40 Tapoi 821 <https://doi.org/10.1007/s11245-018-9626-5> accessed 8 December 2022.
[94] Securities & Futures Commission of Hong Kong, *Regulatory approaches to Authorized Institutions' interface with Virtual Assets and Virtual Asset Service Providers*, (5 September 2017, IOSCO Publishing) <https://www.iosco.org/library/ico-statements/Hong%20Kong%20-%20SFC%20-%20Statement%20on%20initial%20coin%20offerings.pdf> accessed 1 December 2022.

HKSAR are required to apply for a licence under Art 53ZRK, which contains requirements for the granting of a licence for the operation of a VASP. Broadly, they include, AML and anti-terrorism financing policies, compliance with reporting and disclosure obligations, cyber security, appropriate risk management regulations, among others.[95] These form the baseline requirements for VASPs operating in HKSAR. However, Art 53ZRK is not an exhaustive list, and the regulatory authority has the general discretion to consider a myriad of other factors before granting licence for VASPs to operate.

It is similarly worth additionally considering the circular put out by the HKSAR Monetary Authority, which highlighted three core themes for the regulatory approach which HKSAR has been taking with regard to VASPs - supervision, AML and financial crime risk, and investor protections. For the purposes of this paper, only AML provisions will be considered.[96] Under these AML provisions, there are two core obligations which VASPs have to fulfil. First, VASPs are required to require users to engage in DDA activities through their verified bank accounts. This is akin to real-name verification used in South Korea, and identification requirements in Singapore. Second, VASPs are required to maintain business relationships with banks for the purpose of risk-assessments, customer and VASP due diligence, and maintain capital requirements under traditional banking legislations.[97] Such links VASPs to traditional banks, hence allowing greater scrutiny when it comes to user's activities in the realm of DDAs while also giving VASPs the opportunity to tap on the greater resources which these banks have. In that regard, such similarly ensures greater compliance mechanisms with international standards for AML protection.[98] Indeed, there are strong indications that banks would have a greater role to play in the realm of DDAs. Studies around the incorporation of the SWIFT banking network into the realm of DDAs are currently ongoing.[99] However, where the legislation requires VASPs to actively engage with banks, such integration would undoubtedly promote greater information sharing and capacity building to strengthen the overall AML framework.

From this framework, HKSAR's policies towards the AML framework can be said to focus on the implementation of gap-filling mechanisms. Where VASPs act as digital custodians and operate as trading platforms, they often have their own policies and security measures in place to prevent illegal and illicit activities. However, to harmonise these policies with national and international obligations, mutual cooperation and between VASPs and larger institutions would allow VASPs to maintain a level of discretion with their technical

[95] Art 53ZRK(5) Anti Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022.
[96] Hong Kong Monetary Authority, *Regulatory approaches to Authorized Institutions' interface with 1 Providers*, (Government of Hong Kong, 28 January 2022) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220128e3.pdf> accessed 1 December 2022.
[97] Securities & Futures Commission of Hong Kong (n 94).
[98] Financial Action Task Force, 'Easy Guide to FATF Standards and Methodology: Virtual Assets: What, When, How?' (undated, FATF-Gafi) <https://www.fatf-gafi.org/media/fatf/documents/bulletin/fatf-booklet_va.pdf> accessed 1 December 2022.
[99] Practical Law Finance, 'SWIFT Reports: CBDCs and Tokenized Assets Can Integrate into International Financial Ecosystem' (Thomson Reuters Practical Law, 12 October 2022) <https://ca.practicallaw.thomsonreuters.com/w-037-2021?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 30 November 2022.

expertise in the matter, while similarly strengthening the overall regulatory framework. This two-pronged approach is similarly reflected within their policy paper to tap into the existing financial markets worth over US$4.5 Trillion.[100] In that regard, the role of VASPs is thus exemplified within HKSAR's markets, with greater discretion placed upon them.

While the laws around virtual assets and DDAs within HKSAR are certain, the position with sanctions is particularly unique due to its relations with the People's Republic of China ("PRC"). Under the original Sino-British Agreement, HKSAR was allowed a degree of autonomy and independence in their legislative powers.[101] As a result, HKSAR cannot, as its own independent State, unilaterally sanction another. Instead, Chinese foreign policy is adopted. In that regard, the regime for sanctions in Hong Kong falls under the United Nations Sanctions Ordinance (Cap. 537) and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) which covers sanctions imposed under obligations to the United Nations. However, outside of these legislations, there is a dearth in the imposition of sanctions or trade embargos outside of these obligations. Further, it is similarly key to note that these Acts expressly exclude sanctions made against the PRC. Hence, HKSAR should be said to have limited powers in this area.

However, turning to the PRC's foreign policy and their history of sanctions related to DDAs, one would inevitably observe a particularly contradictory position if compared to HKSAR. The PRC has outlawed the use of DDAs in its entirety.[102] Instead, all intangible currencies were replaced by the CBDCs currency known as the "e-CNY".[103] Yet, in HKSAR, CBDCs are excluded from the definition of a virtual asset.[104] Hence, there seems to be a large conflict-of-laws position surrounding the virtual assets which creates legal uncertainty. On one interpretation, one can presume that virtual assets are completely outlawed, with international transactions illegal. On the other through a narrower lens, virtual assets fall outside the scope of the law of sanctions within the PRC. Undoubtedly, the latter position is untenable, and creates numerous gaps in the law for many to bypass sanctions. However, the former position also conflicts with HKSAR's pro-digital asset policies. In that regard, one could perhaps identify that the reason for VASPs to have such wide powers in HKSAR is to allow VASPs discretion to abide by international obligations independent of the domestic laws. Further, where VASPs work with banks who similarly often operate transnationally and across jurisdictions, they would be able to tap onto the regulatory framework in foreign jurisdictions. In that sense, VASPs would be able to tap

[100] Financial Service Treasury Bureau, *Policy Statement on Development of Virtual Assets in Hong Kong*, (October 2022, Government of Hong Kong) <https://gia.info.gov.hk/general/202210/31/P2022103000454_404805_1_1667173469522.pdf> accessed 29 November 2022.
[101] Galvez et al. (n 85).
[102] Cong Yun and Yun Chen, 'The impact of regulatory ban on connectedness of cryptocurrency market' (2022) Applied Economics Letters, <https://doi.org/10.1080/13504851.2022.2141440> accessed 28 November 2022
[103] Jiaying Jiang and Karman Lucero, 'Background and Implications of China's Central Bank Digital Currency: E-CNY' (11 January 11 2021) <http://dx.doi.org/10.2139/ssrn.3774479> accessed 1 December 2022.
[104] Art 53ZRH (2)(a)(i)(A) Anti Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022.

upon international obligations in foreign jurisdictions, and transpose these regulations towards end-users in HKSAR. Hence, the wide discretion which VASP and banks enjoy within HKSAR may be preferable given the unique position which HKSAR has.

As a whole, one can thus sum up HKSAR's position with regards to DDAs as one which is rather broad. HKSAR seems to be looking to prioritise and embrace the technology behind DDAs. The trend seems to follow that they believe VASPs to be in the best position to determine their independent appropriate risk-management for AML and sanction legislations. Hence, the emphasis is placed on private due diligence obligations. Conversely, there are similar obligations for these VASPs to work with larger financial institutions to encourage capacity building in AML, as well as compliance with international law obligations through tapping on these transnational corporations.

2.4 Chinese Taipei

2.4.1 The regulatory framework of DDAs in Chinese Taipei

At first glance, Chinese Taipei seems to be in the same boat as HKSAR - its position in international law is in itself unique and largely complex, enjoying greater autonomy but also greater conflicts with the PRC than that of HKSAR. Beginning with a brief history,, the Qing Dynasty was overthrown by the Kuomintang Party in 1912, led by Chiang Kai Shek. In its wake, they formed the Republic of China.[105] Fast forward to 1927, the Chinese Communist Party declared a civil war against the Kuomintang, forcing them to flee in 1949 to a neighbouring offshore island known as Formosa to establish their own government.[106] Later that year, on 1 October 1949, the Kuomintang declared Formosa as its independent country, under the original banner of the Republic of China, forming Taiwan.[107] However, to this day, the PRC has not recognised this claim; conversely, it forms part of its foreign policy that countries dealing with the PRC should similarly reject recognition of Taiwan, requiring the international community to dub it "Chinese Taipei".[108] Despite the ongoing hostilities and political tension which lasts to this day,[109] the PRC has seemingly left Chinese Taipei largely alone,[110] allowing them to develop their own robust infrastructure through the years.

As a result of this period of autonomous governance, Chinese Taipei has flourished economically, growing to become the 22nd largest GDP in the world boosted by its world-

[105] Xiaoyuan Liu, 'Chiang Kai-Shek's (Invisible) Marathon to the West' (2010) 17(1) Chinese Historical Review 24 <https://doi.org/10.1179/tcr.2010.17.1.24> accessed 30 november 2022.
[106] Michael Lynch, *The Chinese Civil War: 1945-1949* (Bloomsbury Publishing 2022).
[107] ibid.
[108] Christopher Hughes, *Taiwan and Chinese Nationalism* (Routledge Publishing 1997).
[109] Yinghua He, Ulf Nielsson and Yonglei Wang, 'Hurting without hitting: The economic cost of political tension' (2017) 51(C) Journal of International Financial Markets, Institutions and Money 106.
[110] ibid.

class semiconductor industry and innovation incubators.[111] Hence, it is not unfamiliar to the role of modern technological developments. In 2013, merely five years after Bitcoin's release when the asset was only valued at USD $350 each, the central bank in Chinese Taipei was quick to issue a press release indicating that crypto assets will fall under the banner of "virtual commodity".[112] Subsequently that year, banks were disallowed from allowing individuals to trade crypto-assets.[113] In that regard, the early years saw a significant degree of scepticism towards the use of these assets by Chinese Taipei. This scepticism has seemingly carried over to the modern era, where the economy has recently announced plans to disallow the purchasing of cryptocurrencies with credit cards.[114] In that regard, one inevitably sees the reluctance of the economy to engage in this novel financial technology.

It was, however, only recently in 2019 at the Asia Blockchain Summit, that Taiwenese legislator Jason Hsu announced the country's plans to become a "crypto-nation".[115] Following that announcement, Chinese Taipei revamped its legislation completely, introducing a new framework for DDAs in the country. Indeed, VASPs within the region were governed to fall under the broader term "financial institutions" under the amendments to the Money Laundering Control Act ("MCLA"). Under Art 5, this placed VASPs in the same operating conditions as traditional banks, requiring them to implement internal control and audit systems, risk assessment reports, as well as traditional AML and terrorist financing legislation.[116] Particularly notably however, there are no specific rules or regulations for VASPs to be registered or licensed in Chinese Taipei; instead registration and licensing requirements for VASP fall under the general requirements for financial institutions.[117] Instead, the position when it comes to DDAs within Chinese Taipei is largely focused on supervision of AML and sanction-compliance, rather than overall regulatory oversight.[118]

Unfortunately, apart from this Chinese Taipei's position around DDAs, as well as an overall taxonomy of DDAs the issue seems rather lacklustre. The government has made no

[111] John Mathews and Mei-Chih Hu, 'Enhancing the Role of Universities in Building National Innovative Capacity in Asia: The Case of Taiwan' (2007) 35(6) World Development 1005
[112] UK Jurisdiction Taskforce (n 37).
[113] ibid.
[114] Sandali Handagama, 'Taiwan Set to Ban Crypto Purchases Using Credit Cards: Report' (22 July 2022). <https://www.coindesk.com/policy/2022/07/22/taiwan-set-to-ban-crypto-purchases-using-credit-cards-report/> accessed 29 November 2022.
[115] Rachel Wolfson, 'Crypto Congressman Jason Hsu On Taiwan Becoming A Blockchain Island And Crypto Nation' (*Forbes*, 29 August 2018) <https://www.forbes.com/sites/rachelwolfson/2018/08/29/crypto-congressman-jason-hsu-on-taiwan-becoming-a-blockchain-island-and-crypto-nation/?sh=4490a0ec49b7> accessed 3 December 2022.
[116] For a translated version, accessed at <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131> accessed 6 December 2022.
[117] See, a list of 24 VASP service providers licensed under the rules for financial institutions at <https://www.fsc.gov.tw/userfiles/file/(111_9_2更新)已完成洗錢防制法令遵循聲明的虛擬通貨平台業者名單.pdf> accessed 2 December 2022.
[118] Cheng Hwa Lee, Heng-Li Yang and Shiang-Lin Lin, 'The Key Evaluation Criteria of Blockchain Technology Implementation' (2021) 24(4) 科技管理學刊 [Journal of Science and Technology Management] 1

indication on establishing a formal definition for DDAs, but rather has taken a negative approach to define security tokens, and having everything outside its scope to form "virtual commodities".[119] More recent legislation in the 2021 Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction ("RGAVCT") similarly takes a broad approach. In particular, Art 2(2) reads:

> 2. "A virtual currency" refers to a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes. However, virtual currencies do not include digital representations of NTD, foreign currencies, currencies issued by Mainland China, Hong Kong, or Macao, securities, and other financial assets issued in accordance with laws.

This definition is particularly broad and general, not really reflecting the nuances of DDAs, instead, placing great emphasis on the technology which is used in the issuance of these assets. However, there are greater nuances when it comes to DDAs. For instance, CBDCs which run on these technologies are inherently covered by this legislation despite having a fundamentally different characteristic entirely, and treated differently across other jurisdictions. This trend seems to follow the publicity which the Taiwanese media has given to DDAs, where a majority of its comments around DDAs were made around the umbrella term of cryptocurrencies such as Bitcoin, rather than modern developments surrounding DDAs.[120] As such, and perhaps owing to the general infamy of cryptocurrencies,[121] the full nature of DDAs has not been fully appreciated by the economy. Even domestic commentators have called for more robust developments in the field of DDAs.[122] Hopefully however, this would similarly serve as a wake up call for the economy to better develop its DDA-based infrastructure, less it gets left behind by the rest of the region.

In that regard, one can say that the Chinese Taipei economy still seems to be finding its footing and position over the application of DDAs. While certain members of the

[119] Abe Sung, Eddie Hsieung, 'Cryptoassets & Blockchain in Taiwan' (*Lexology*, 19 December 2019), <https://www.lexology.com/library/detail.aspx?g=75c285a8-d738-4052-b1a3-bcface3d31d4> accessed 2 December 2022.

[120] Hsin-Ke Lu and others, 'A study on adoption of bitcoin in Taiwan: using big data analysis of social media' (International Conference on Communication and Information Processing, November 2017), 32. <https://doi.org/10.1145/3162957.3163046> accessed 3 December 2022.

[121] Gourang Aggarwal and others, 'Understanding the Social Factors Affecting the Cryptocurrency Market' (International Conference for Internet Technology and Secured Transactions). <https://doi.org/10.48550/arXiv.1901.06245> accessed 1 December 2022.

[122] Editorial, *Nation lags world in crypto controls* (21 November 2022), <https://www.taipeitimes.com/News/editorials/archives/2022/11/21/2003789312> accessed 2 December 2022.

legislature might be intrigued by the idea of embracing these new technologies,[123] the overall position seems to indicate significant reluctance of incorporating DDAs into the general economic ecosystem. Hence, it would seem that Chinese Taipei has a limited role in DDAs.

2.4.2. AML laws and economic sanctions of DDAs in Chinese Taipei

While not much can be said surrounding the treatment by regulators and policymakers in Chinese Taipei, their focus on AML provisions is nothing to scoff at. Indeed, the treatment of VASPs under the wider category of financial instruments undoubtedly allows the economy to use a tried and tested system for the regulation of this new industry.[124] Such similarly allows for a more certain legal framework, for both legislators and lawyers with experience in this field, but also for end-users who would be familiar with these legislations.

The current MCLA framework for financial institutions in Chinese Taipei imposes the following obligations against Financial Institutions:

1. Maintenance of records of transactions (Art 8), alongside reporting obligations (Art 9)
2. Reporting suspicious transactions (Art 10)
3. International cooperation (Art 11)

It must be emphasised that these regulations are not unique to DDAs, but apply to all financial institutions operating in the economy. What seems intriguing however, is that these provisions fall into a similar category as the legislation put by Singapore. In essence, by grouping VASPs together with financial institutions, it promotes a top-down governance of DDAs, which seems to frustrate the notion of "decentralisation" of these assets. For instance, in the maintenance of records and transactions, Art 8 of the MLCF is particularly detailed to require financial institutions to maintain these transactions for "at least five years". However, it is silent on the methods of record keeping, instead, looking to "consult with relevant industry associations" to determine the scope of the record. For DDAs however, this may create significant controversy over the scope of the records, and whether they would include an individual's personal and sensitive information. In that sense, two conflicting approaches can be adopted: first, full disclosure of these personal information, using real world verification data obtained under due diligence provisions under Art 7. Alternatively, it could adopt the position of South Korea, and record the unique wallet addresses to preserve individuals' data, and only match wallet details to real world data when a transaction is deemed suspicious. In that regard, there is a significant degree of uncertainty in the strength of AML laws in Chinese Taipei.

[123] UK Jurisdiction Taskforce (n 37).
[124] Under Article 5(2) of Money Laundering Control Act, there is an express requirement that virtual asset service providers are subject to similar rules and regulations as traditional financial institutions.

There was an effort to answer these questions by Chinese Taipei. Art 7(1) of the RGAVCT specifies that customer due diligence includes a reporting of the transactions from both the originating party, and the beneficiary. Art 7(2) then goes further to explain that the official national identification number, address, date and place of birth, and wallet information should be included in the report. This is indeed a positive first step for regulatory initiatives for DDAs in Chinese Taipei. However, the questions regarding the extent of the reports submitted to the relevant authorities, whether the specific transaction chain, or the entire transaction history of an individual deemed suspicious, remains unanswered. Further, the legislation is similarly silent on how this personal information would be treated by the relevant authorities. In that sense, one can conclude that the Taiwanese position is similar to that in Singapore.

A further comment should be made about the role of sanctions by Chinese Taipei, especially given its unique position in international law. Unlike HKSAR, Chinese Taipei has its own independent regime of enforcing sanctions. Most recently, following the Ukrainian invasion, Chinese Taipei has imposed similar sanctions to the Western world,[125] whereas the PRC has remained silent and neutral on the issue. Similarly, it seems evident that Chinese Taipei is acting compliant with UNSC sanctions, despite the region not being part of the international organisation.[126] While it is hopeful that Chinese Taipei is independently to be following the trends and ensuring compliance in international law despite being in a grey area itself, the dearth of literature, coupled with partial recognition of the State,[127] indicates that the imposition of sanctions are largely voluntary.

The law however, is equally murky when it comes to DDAs in Chinese Taipei. Not only is the MCLA silent on the position of sanctions, especially with regard to DDAs, but there seems to be a dearth in the legislative action surrounding sanctions of DDAs in Taiwan. The only reference to "sanctions" can be found in Art 4(7) of the RGAVCT, that prevents VASPs or DDA custodians from engaging in business relations with organisations under the Counter-Terrorism Financing Act. However, Art 4 of this Counter-Terrorism Financing Act merely focuses on targeted sanctions, as opposed to general trade sanctions made against another sovereign nation. In that sense however, one can make a reasonable assumption that under Art 4(7) of the RGAVCT, the cessation of business relationships would extend to individuals or organisations of a sanctioned country. This interpretation should follow Art 1 of the Counter-Terrorism Financing Act on the purpose of sanctions in general, namely, the "[preservation] of international security, [and the protection of] fundamental human rights".

[125] Ministry of Foreign Affairs fort the Republic of China (Taiwan), *The Republic of China (Taiwan) government strongly condemns Russia's invasion of Ukraine in violation of the UN Charter, joins international economic sanctions against Russia*, (25 February 2022, Government of the Republic of China (Taiwan) <https://en.mofa.gov.tw/News_Content.aspx?n=1328&s=97420> accessed 2 December 2022.
[126] Reuters Staff, *Taiwan tells U.S. it is complying with North Korea sanctions,* (19 May 2020 Reuters). <https://www.reuters.com/article/us-northkorea-missiles-taiwan-usa-idUSKBN22V0F6> accessed 3 December 2022.
[127] Randall Newnham, 'Embassies for Sale: The Purchase of Diplomatic Recognition by West Germany, Taiwan and South Korea', (2000) 37 International Politics, 259.

As a whole, it is rather unfortunate that there is a significant dearth of legislative action around the role of DDAs within Chinese Taipei. However, it seems only recently that the legislature has shaken off its regulatory chill and begun to realise that greater work needs to be done across DDAs in the country. Nonetheless, the current trend surrounding the regulatory action in the country seems rather similar to Singapore, emphasising a more top-down approach towards DDAs in the region.

3 A comparative view

Before delving into this analysis, it is helpful to give a summary of the positions of these economies with regards to DDAs. From the analysis above, Singapore seems to be taking the most heavy-handed approach towards regulating DDAs, treating them as yet another asset with its top-down obligations on users as well as VASPs (or digital payment token services as known there). However, the other economies seem to be embracing the decentralisation and technology behind these assets, giving VASPs wider discretion. Of note, HKSAR and South Korea have seemingly taken up a "minimum core obligations" approach, leaving much discretion towards VASPs to regulate their own behaviour while imposing a minimum standard for them to adhere to. HKSAR has even gone a step further to impose an obligation for VASPs to work with established financial institutions to promote mutual capacity building measures. Conversely, Chinese Taipei's regulatory environment for DDAs seems to currently be in its infancy; requiring VASPs to abide by traditional rules which govern financial institutions. However, it is hoped that the Digital Assets Act 2023 in Chinese Taipei will clear the air and bring some clarity to the field soon.

Utilising this, this section will delve into a comparative analysis of how DDAs are treated within their jurisdictions, and their interactions with the beginnings of international law in DDAs. In particular, it focuses on the three areas which it identified - the taxonomy, internal policies, and compliance with international AML obligations. In that regard, a key overarching theme in the following analysis will be the interaction of these independent legislations within the wider regional, and international DDA and AML frameworks. While it notes that the disharmony surrounding DDAs seems particularly worrying, the current reality of DDAs makes this fear largely unfounded.

3.1 Taxonomy of DDAs

As with each snapshot of each country, this section will begin first to compare and analyse the framework of each nation's treatment of DDAs. Such a comparison will allow one to determine if there are legislative gaps in the framework surrounding DDAs, and potentially point out areas where there is an inconsistency with the laws surrounding DDAs alongside its international obligations. Having already considered the individual position of each economy, this section will first begin with the definition adopted by the international

community. Namely, the United Nations International Institute for the Unification of Private Law ('UNIDROIT'). Under their Working Group 3, the definition which they have adopted can be found across 'Category 1' and Category 2' based DDAs.[128] They include:

> **Category 1**: transferable code constituting a representation of:
> (i) a moveable tangible
> (ii) an immovable tangible
> (iii) a tokenised currency, of which two fundamentally distinct categories
> - privately tokenised fiat funds (e.g., the utility settlement coin)
> - central bank digital currency (CBDC)
>
> (iv) an intangible financial asset
> (v) an intangible non-financial asset (e.g., IP)
>
> **Category 2:** transferable code constituting a representation of an asset that is not a Category 1 asset.[129]

Examples of Category 1(iii) assets under UNIDROIT's definition include the Utility Settlement Coin project by Fnality.[130] Examples of Category 2 assets include Bitcoin, and Non-Fungible Tokens ('NFTs'). However, the UNIDROIT working group noted that there is a further third category of 'stablecoins' which was not reflected, listing examples including KPM Coin, Diem, and Dai (MakerDAO).[131] There is similarly an additional category which UNIDROIT has mentioned in their working paper, but not expressly codified - a category 3 for Stablecoins.[132] However, there is some confusion over how this new category would operate, compared to "privately tokenised fiat funds". Considering these crypto-assets with a different framework from stablecoins (under the proposed Category 3) even though they serve similar purposes only creates confusion. However, this category 3 presently does not stand, and stablecoins fall under the provisions laid out in Category 1.[133]

There are three core distinctions with the definition laid out by UNIDROIT, and the interpretation of DDAs by these nations. First and importantly, the UNIDROIT working paper expressly acknowledged that CBDCs form part of the umbrella of DDAs. Conversely, three of the Four Asian tigers (missing Chinese Taipei) excluded CBDCs from their definition of DDAs. This position adopted by them seems preferable. While CBDCs may be

[128] United Nations International Institute for the Unification of Private Law, Digital Assets and Private Law Working Group, Issues Paper, Study LXXXII – WG3 – Doc 2 (rev 1), adopted 2 July 2021
[129] ibid 54.
[130] See at <https://www.fnality.org/home> accessed 2 December 2022. Discussed in (n 140), 40.
[131] ibid 57-8.
[132] ibid.
[133] ibid 40.

decentralised,[134] they do not have the same risk profile as DDAs for AML provisions. First, CBDCs are issued by the State, and often backed by a fiat currency - the State's national currency. Where these tokens are issued by the States, States can program AML safeguards within them that would be unseen to the naked eye.[135] Such has indeed already been implemented in other State-distributed DDAs. Decentralised and tokenised green bonds from Project Benja have safeguards to ensure that the funds are only used for their purpose as a blockchain-based carbon credit scheme.[136] In that regard, the programming of internal AML measures such as mechanisms to track the currency would be possible.[137] As such, the position of Singapore, South Korea and HKSAR is undoubtedly preferred. CBDCs should not fall under the traditional scope of DDAs in the law of sanctions.

Second, DDAs within UNIDROIT's framework includes decentralised securities under Category 1's "digital representation of a movable tangible". This seems to include commodity backed tokens as well as digital securities; a distinction was not made within the UNIDROIT working papers.[138] Conversely, across the Four Asian Tigers, there have been express provisions made where decentralised securities fall outside the scope of DDA provisions, and are instead governed under the same traditional categories as non-digital securities. At this juncture, it is hence worth noting that nations have been working together with the International Council of Securities Association ("IOSCO") to put forth developments across DDA security-based legislations.[139] Indeed, the IOSCO has been working with various nations, including the Four Asian Tigers, on developing a harmonised framework in the realm of security-based DDAs.[140] Similarly, one can thus assume that UNIDROIT will soon take a step back in this field, given that the organisations have a long history of cooperation in this field.[141] However, further consideration by the IOSCO should be given to existing frameworks, such as the UNIDROIT Convention on Substantive Rules for Intermediated Securities (2013) and the UNIDROIT Legislative Guide on Intermediated

[134] For instance, as discussed by the Central Bank of Malaysia in: Nurjannah Ahmat and Sabrina Bashir, 'Central Bank Digital Currency: A Monetary Policy Perspective' (September 2017, Central Bank of Malaysia) <https://www.bnm.gov.my/documents/20124/826874/CB_Digital+Currency_Print.pdf> accessed 2 December 2022.
[135] For instance, as discussed by the European Union in: European Central Bank, *Exploring Anonymity in Central Bank Digital Currencies*, (December 2019, Issue 4 - In Focus, Eurosystem). 5-9 <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf> accessed 6 December 2022.
[136] Monetary Authority of Singapore (n 41).
[137] Bank for International Settlements, 'Central Bank Digital Currencies: System Design and Interoperability', (September 2021, Report 2, BIS Publishing) <https://www.bis.org/publ/othp42_system_design.pdf> accessed 3 December 2022.
[138] Reuters Staff (n 126), 27, 81.
[139] Jane Diplock, 'Securities Regulation - An International Perspective' (International Council of Securities Association, Tokyo, 30 October 2006). <https://www.iosco.org/library/speeches/pdf/securities_regulation_international_perspective_oct06_jd.pdf> accessed 3 December 2022.
[140] International Council of Securities Association, *IOSCO Decentralised Finance Report*, (March 2002, OR01/2022, IOSCO) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf> accessed 2 December 2022.
[141] Rita Cunha, *Memorandum of Understanding (MMOU): An international Benchmark for Securities Enforcement*, (UNIDROIT Colloquium, 6-7 September 2010, UNIDROIT Secretariat). <https://www.unidroit.org/english/documents/2010/study78b/cem1-colloquium2010/cunha.pdf> accessed 4 December 2022.

Securities (2017). As such, one can thus expect the IOSCO to begin leading the field in this area; a consensus among the Four Asian Tigers towards their stance on DDAs is, in itself, thus promising.

Lastly, and particularly within the realm of DDAs, a word has to be said about the non-specificity of UNIDROIT's classification with regard to Category 2 assets. UNIDROIT's current position seems to best reflect the position in Chinese Taipei - the 'catch-all umbrella' category consisting of everything that is not a digital asset; a similar trend appears to be present where Category 2 assets were only described as including Bitcoin, or NFTs; more broadly speaking, assets which have seemingly garnered the most infamy and media attention.[142] Conversely, Singapore, South Korea and HKSAR all contain a more robust definition of DDAs within their national legislation. The importance of such a distinction indicates a broader and more nuanced understanding of these assets, which is similarly evident in subsequent legislation concerning digital payment tokens, virtual assets and virtual commodities respectively. In a practical setting, this disharmony would create a degree of legal uncertainty. End-users, investors and even issuers of DDAs would have to understand different nuances in classification of assets, and comply with different regulations as they operate in different regions.

As such, one can thus see the consequences surrounding a non-harmonised taxonomy of DDAs. Unfortunately, it seems that domestic legislations seem to be more robust, and have greater overall certainty as compared to their international counterparts. However, to achieve a strong overall framework and consistent regulatory environment for DDAs as they often operate in a transboundary setting, there needs to be a clear and consistent use of taxonomy for DDAs. Currently, it seems that only three out of the four powerhouses in the region are fully ready to embrace these assets.

3.2 Treatment of VASPs

DDAs are not the only matter which requires legal certainty. VASPs, and DDA custodians have a similarly large role to play in the regulatory process. After all, end-users would not be able to access their virtual commodities or virtual assets without a platform or interface, given the intangible nature of these assets. Indeed, for beneficiaries and receivers of DDAs, the crux of the mechanism which they utilise these assets lies in the conversion of intangible financial instruments, with tangible physical objects used to commit wrongful acts.[143] Hence, where VASPs act as the gatekeeper towards enforcing AMLs, the regulatory framework surrounding them should be discussed.

[142] Hwa Lee (n 118).

[143] See here, for example, the status of Russian Paramilitary Groups using digital assets to evade sanctions in: Peter Maroulis, Nick Grothaus and James Disalvatore, 'Online Crowdfunding Campaigns use Cryptocurrency to Support Russian Paramilitary Groups in Ukraine' (5 December 2022), <https://brief.kharon.com/updates/online-crowdfunding-campaigns-use-cryptocurrency-to-support-russian-paramilitary-groups-in-ukraine/> accessed 6 December 2022.

In the current international framework, the Financial Action Task Force ("FATF") has been working with UNIDROIT towards a regulatory framework. Generally regarded as the organisation in charge of international AML standards,[144] the FATF has been seeking to harmonise the laws surrounding DDAs globally. However, what is interesting is that within UNIDROIT Working Papers, the FATF has made a distinction between "tradability" of assets, and the "transfer of assets", going at odds with the UNIDROIT Secretariat.[145] This position was subsequently reflected within FATF[146] and UNIDROIT[147] reports - while 'trade' was defined as the exchanging of the intangible for a tangible, or recognised legal tender, 'transfer' refers to the exchange of digital assets from an originator to a beneficiary. Such a particularly nuanced view exemplifies the role of VASPs within the DDA ecosystem. In that light, the FATF has taken centre-stage in attempting to develop an international regulatory framework of VASPs.[148] Unfortunately, this important distinction seems to have been lost in translation within the legislative framework across the Four Asian Tigers, each treating them as one and the same term. However, such a distinction is particularly relevant in AML laws where the whole purpose of utilising DDAs is founded on a means of "cleaning dirty money". In that aspect, Singapore's heavy top-down approach can thus be said to be more effective in this last-leg, whereas South Korea, Chinese Taipei and HKSAR's more discretionary approach is better suited to facilitate transfers in DDA-based investments.

A second consideration lies in the risk-assessment framework posited under FATF guidelines. In essence, VASPs traditionally focuses on risk assessments of DDAs, customer due diligence, VASPs maintaining banking relationships, implementation of the "travel rule", internal controls, harmonising policies across foreign branches, reporting of suspicious activities and mechanisms for whistleblowing, as well as mutual cooperation across VASPs.[149] This is a particularly extensive set of top-down obligations which the FATF seems to impose on VASPs, which are consistent with many of the provisions found within these economies. Nonetheless, they seem to be largely harmonised under both FATF guidelines, as well as across the economies in the Four Asian Tigers. For instance, customer due diligence obligations across the four jurisdictions is largely harmonised with principles set out by the FATF - namely, that all end-users should disclose personal information to VASPs when using the data. Interestingly however, one area which all

[144] Navin Beekarry, 'The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law' (2011) 31 Northwestern Journal of International Law and Business 137.
[145] Digital Assets and Private Law Working Group, *Summary Report of the First Session*, Study LXXXII – W.G.1 – Doc. 4 (rev. 1), 17-19 November 2020. United Nations International Institute for the Unification of Private Law.
[146] Financial Action Task Force, *Virtual Assets and Virtual Asset Service Providers, Updated Guidance for a Risk-Based Approach* (October 2021, FATF/OECD) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 2 December 2022.
[147] Digital Assets and Private Law Working Group, *Master Copy of the Principles and Comments*, Study LXXXII – W G 5 – Doc 3 (rev 1) 7-9 March 2022, United Nations International Institute for the Unification of Private Law.
[148] ibid. Also note that UNIDROIT seems to be silent on the role of VASPs within their work.
[149] Beekarry (n 144).

jurisdictions have left to the discretion of VASPs lies in the mechanisms of their reporting obligations. This is in line with the FATF report, which seems to embrace various mechanisms for implementing AML reporting procedures.[150] However, guidelines have been provided in the consultation paper on red-flag indicators for VASPs to utilise.[151] Nonetheless, these guiding principles provide a strong framework for VASPs to tap upon, and to utilise as guidance, even if they are not bound by these principles. As such, one should applaud this extensive framework which the FATF recommends looks to mitigate and minimise any potential risk which may arise through DDAs.

However, it should also come as no surprise that there are definitely varying degrees of implementation of these standards. Singapore currently has the greatest "top-down" regulatory approach towards VASPs, complying with FATF guidance and even going further than that with reporting and record-keeping obligations imposed on VASPs operating in Singapore include mandatory periodic disclosure obligations.[152] While the FATF is currently silent on this, it instead adopts a "wait-and-see" framework where third party supervisors may request for certain information at given points in time.[153] Conversely, HKSAR, South Korea and Chinese Taipei are attempting to preserve anonymity, and, in line with standards set out by the FATF, only request for information when required. Such over-preparedness by Singapore might be detrimental for the use and growth of DDAs within Singapore, where anonymity in transactions has become a fictitious concept despite international standards not requiring such disclosure. Yet, having the relevant authorities hold information at the ready might similarly allow for the strengthening of AML obligations through more timely responses. This presents a precarious balancing act which would undoubtedly determine the future of DDAs in Singapore, and whether they would be widely adopted. Despite this disharmony however, the minimum obligations can be said to have been met.

Unfortunately, a word has to be said about the disharmony across capacity building obligations, and varying degrees of trust that central authorities take towards these VASPs. Currently, only South Korea, HKSAR and Chinese Taipei give VASPs a significant amount of discretion in their operation, merely providing requirements for the end goal of AML laws. This follows the position of the FATF, which similarly place an emphasis on promoting cooperation within the private Sector. Indeed, the FATF has even provided express recommendations which promote mutual capacity building and information sharing between VASPs and Banks.[154] Conversely, Singapore has taken a more regulatory approach towards defining each individual obligation, distinguishing them as a unique

[150] ibid 88.
[151] Financial Action Task Force, '*Virtual Assets, Red Flag Indicators of Money Laundering and Terrorist Financing*' (September 2020, FATF/OECD) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf> accessed 3 December 2022.
[152] Cf s.16(3) of the *Finance and Securities Market Act* 2022.
[153] Beekarry (n 144), 104 [7].
[154] ibid 82, 102.

entity in the market across seven different categories[155] Such a disharmonised framework is rather problematic, particularly when there are disparate standards which result due to developments in technology. Indeed, if too much regulatory oversight is imposed in the technological standards which these nations adopt, there would be concerns that VASPs lack discretion to upgrade their security framework in line with corporate standards. The situation is particularly worse for VASPs which operate exclusively in Singapore, where they would have no obligations to update their AML or protection frameworks, nor have foreign branches which they can tap on. This latter point is similarly made worse given the particularly onerous obligations Singapore imposes on VASPs operating transnationally.[156] As such, too much regulatory oversight would inherently leave VASPs operating in Singapore at a different technological standard from the rest of the region.

Such a disparate technological standards would, if left unchecked, lead to issues both within DDA technologies itself, as well as disharmonised regulatory standards. On the former, "splitting" within DDAs occurs where significant holders of a particular asset become incompatible with the larger pool of assets. This results in the particular asset splitting into two distinct forms of currencies, with these incompatible assets becoming its own unique currency. This was the case for Ethereum's hard fork, resulting in two different cryptocurrencies of Ethereum and Ethereum Classic.[157] Such incompatibility due to disparate technological standards might be cause for concern. On the latter, greater regulatory oversight over the operating standard of VASPs might similarly result in a stagnation of AML frameworks in these VASPs where top-down approaches do not adapt. Such further fragments the standards of VASPs within the region, creating an overall disharmonious technological framework.

Finally, the technical aspect surrounding DDAs and the importance of VASP's due diligence obligations should be discussed. At present, all four economies have obligations for VASPs to conduct due diligence studies on the particular DDA which they wish to offer; albeit to varying degrees. However, what is common between them, is that the core due diligence obligations seem to be merely limited to customer and beneficiary due diligence; only HKSAR imposes an additional obligation for VASPs to understand the underlying asset which they are offering. This obligation to understand the asset however, is of particular importance. While there is established precedent of DDAs being programmed to be able to fund projects which ensure public good, such as within the trading of smart carbon credits,[158] the reverse can similarly be done. Various organisations can issue DDAs programmed to fund wrongful conduct, such as the purchasing of arms in sanctioned

[155] Lim Chong Kin, Benjamin Gaw and Elizabeth Tong, 'Singapore' in Barbara Stettner and Bill Satchell (eds), *Global Legal Insights Fintech* (Global Legal Group Publishing 2019) 218.
[156] ibid 219-20.
[157] Chitturi Prasad and others, 'Quantifying Blockchain Immutability Over Time' (5th International Conference on Electronics, Communication and Aerospace Technology 2021) 715,720 <https://ieeexplore.ieee.org/abstract/document/9675947/> accessed 1 December 2022.
[158] Project BENJA and Project Genesis (n 3).

countries. In that regard, without proper due diligence on the asset, DDA issuers could potentially hide their malicious intentions within the code of the asset that is often overlooked by investors. This emphasis on the use of technology to bypass assets is not a novel concept, and has seen discussion across applications which are predominantly used by DDA-based investors.[159] In particular, the messaging platform "Telegram" has garnered a notorious history of being used to bypass sanctions.[160] As such, while the due diligence obligations within these economies are a good first step, HKSAR seems to be leading the field in this aspect.

Overall, the rules surrounding VASPs are rather broad and currently disharmonised across the region. Indeed, there are significant efforts to implement the international guidance provisions by the FATF to strengthen AML laws. However, where a country's attitude towards VASPs remains particularly top-down, there is a concern that these regulations would fall behind corporate standards, particularly when the rest of the region seems to be embracing these matters. As such, this disharmony in technological standards may become cause for concern going forward.

3.3 Compliance with international law obligations

The final area for consideration lies in the role of international law obligations which States have. In the area of AML and economic sanctions, this generally takes the form of compliance with UNSC resolutions in imposing sanctions against individuals, or general trade sanctions against nations. There is, unfortunately, no general framework for the imposition of unilateral sanctions against particular nations.[161] As such, compliance with international law obligations pertaining to sanctions is difficult to assess. This is especially true for HKSAR and Chinese Taipei, due to their political difficulties in assessing their foreign policies in light of pressures by the PRC. Hence, this subsection will primarily consider the application and enforcement of sanctions ordered by the UNSC.

From the snapshot of the Four Asian Tigers, it is particularly evident that they do comply with the relevant UNSC sanctions, and have mechanisms in place to enforce a sanctions regime. However, UNSC sanctions are traditionally more targeted, rather than operating as general trade sanctions.[162] This is largely owed to their design to prevent a State's continuous wrongful conduct, aiming to stem the means to their ends.[163] Oftentimes, the

[159] Leonardo Nizzoli and others, 'Charting the Landscape of Online Cryptocurrency Manipulation' (2020) 8 IEEE Access 113239-113245.
[160] Ehsan Lor Afshar, 'Banking the Bazl: Building a Future in a Sanctioned Economy' (2022) 9(1) Economic Anthropology 60.
[161] Marc Bossuyt, 'Consequences of Economic Sanctions on the Enjoyment of Human Rights' (2000, E/CN 4/Sub 2/2000/33, UN Sub-Commission on the Promotion and Protection of Minorities). [5] <https://www.ohchr.org/sites/default/files/Documents/Events/WCM/MarcBossuyt_WorkshopUnilateralCoerciveSeminar.pdf> accessed 1 December 2022.
[162] Francesco Giumelli, 'Understanding United Nations Targeted Sanctions: An Empirical Analysis' (2015) 91(6) International Affairs 1351 <https://doi.org/10.1111/1468-2346.12448> accessed 29 November 2022.
[163] ibid.

nature of these targeted sanctions, targeting a particular industry, would be easier to enforce. However, the opposite is true for DDAs. The current framework means that such targeted sanctions would allow DDAs to inherently fall through their provisions, particularly when they have a peer-peer framework. Hence, even with real-world verification measures, there would be no oversight actively preventing the transfer of DDAs into sanctioned countries. Especially if real world verification is only one-sided, VASPs and regulators would be unable to track the subsequent movement of DDAs once transferred to a country with a more lax regime. Following, DDAs can then be exchanged for tangible goods at a later stage once within the ecosystem of sanctioned countries, subsequently bypassing sanctions. The situation is especially worse when there is, at present, no international framework for VASPs to comply with. Indeed, all current legal obligations for VASPs and DDAs stem from the economies which they are operating in. Even if they were to trickle down from the international level at a later stage, it might still take time for States to legislate these international obligations into domestic law, and ensure VASP compliance. Hence, targeted sanctions, while potentially effective at the international level, might be inadequate if a framework governing DDAs are to be applied.

Despite these matters, the work of all Four Asian Tigers in the realm of economic sanctions is undoubtedly to be applauded. Singapore, in particular, has attempted to circulate advisors to ensure that VASPs do take note and be wary of the role of international sanctions, urging VASPs to prevent transactions to locations with IP addresses indicating sanctioned country.[164] Conversely, South Korea, HKSAR and Chinese Taipei have not made any statements surrounding the enforceability of these sanctions within the realm of DDAs. However, it would seem that as the remaining economies do have significant regulatory plans in the works, set to be enacted very soon. In that regard, it is hopeful that greater clarity on the interaction between DDAs and domestic regimes will come into play; even expressing references and acknowledgements of the transboundary nature of these assets would allow international law to take its roots within DDAs.

4 Towards a harmonised framework

Having identified the issues, this paper then seeks to set out solutions and guidance towards a harmonised regulatory framework. To that end, two principles can be tapped upon - that of comity between regulators, as well as mutual cooperation with the private sector.

[164] Monetary Authority of Singapore, *Guidelines to MAS Notice PS N-02 on Prevention of Money Laundering and Counter-terrorism Financing of Terrorism*, (16 March 2020, Government of the Republic of Singapore) <https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines-to-PSN02-on-Prevention-of-Money-Laundering-and-Countering-the-Financing-of-Terrorism--DPT.pdf> accessed 2 December 2022.

Beginning first with comity, the role of international comity within digital assets is quintessential due to its fundamentally transboundary nature. In essence, international comity is the mutual respect between political and legislative entities across nations.[165] This includes decisions in both the judiciary,[166] as well as various legislative bodies. Indeed, the role of comity within the laws of DDAs cannot and should not be understated for various reasons. First, DDAs are inherently transboundary in nature. As such, they cannot be said to solely operate within each jurisdiction independently of each other. Conversely, there is an entire ecosystem of DDAs which would be affected by one economy's actions which may have an entire spillover effect within the industry. For instance, when the PRC made an announcement to ban the use of crypto-assets within its country, its value had plummeted drastically.[167] With an understanding of the volatility of these assets, such presents clear evidence that the unilateral action of one economy will frustrate the efforts of the global economy towards mitigating the risk-factor within these DDAs. Hence, the role of international comity cannot be stressed enough.

Undoubtedly, there exists a range of issues where the Four Asian Tigers practise international comity outside of DDAs. For instance, there has been discussion of the harmonisation of civil procedure rules, particularly across transboundary commercial disputes.[168] Similarly, the harmonised compliance with international law obligations is, in itself, a respect for the international legal order along the lines of comity. On this basis, it would be up to the economies to begin consultations with each other to best tackle the issue of DDAs within the region. Certain key themes of the talk should include the harmonisation of due diligence requirements for VASPs, both with regards to customer and DDA due diligence, the harmonising of licensing requirements for VASPs, as well as mechanisms to enhance and promote cross-border real world verification, particularly within the end-user experience (i.e. would both the originator and receiver of DDAs be able to view the others' personal data during the transfer, or merely be limited to the wallet addresses). In that regard, there is significant potential for mutual cooperation by policy-makers to determine the scope of a harmonised DDA framework within the region.

The same can be said for the adherence of DDAs to international standards. While there may be discussion of whether DDAs would fall under targeted sanctions by the UNSC or other international organisations, these economies should instead look towards integrating technologies in the interpretation and enforcement of these orders. This could be achieved through mere treaty interpretation standards, such as those suggested by

[165] Bryan Garner, *Black's Law Dictionary* (10th ed, Thomson Reuters Publishing 2014) 342.
[166] See, for instance, in: E*coBank Transnational Inc v Tanoh* [2015] EWCA Civ 1309, [2016] 1 WLR 2231 where the judiciary gave respect for exclusive jurisdiction clauses and did not want to frustrate the purpose of foreign judiciaries in granting an anti-suit injunction.
[167] BBC Editorial, 'Bitcoin falls further as China cracks down on crypto-currencies' (*BBC News*, 19 May 2021) <https://www.bbc.com/news/business-57169726> accessed 1 December 2022.
[168] James Spigelman, 'International Commercial Litigation: An Asian Perspective' (2007) 37 Hong Kong Law Journal 859.

Anja Ipp through Art 31(3)(c) of the Vienna Convention on the Law of Treaties,[169] which similarly applies within UNSC resolutions.[170] While Singapore has been noted to be leading the charge, South Korea, HKSAR and Chinese Taipei could similarly look towards Singapore as precedent for adopting such a wide view of sanctions and DDAs.

Secondly, and perhaps more briefly, the integration of corporate standards and the future proofing of regulatory work remains quintessential towards long term sustainability of AML mechanisms. While this notion has been briefly alluded to initially with respect to the FATF standards, more can definitely be done. The first step has already been taken by South Korea and HKSAR in embracing these technologies, giving appropriate discretion towards VASPs. HKSAR has even gone further to have VASPs work with larger financial institutions. Singapore and Chinese Taipei should thus look to these economies, and this is the first step towards developing a more robust and sustainable framework through the corporate world.

However, to proceed beyond this and move towards a harmonised framework, regional cooperation between financial institutions, central banking authorities, as well as VASPs need to move beyond a domestic level. Within this, a framework for inter-VASPs cooperation is quintessential to ensure that all VASPs are operating under similar regulatory standards, while giving them a platform to innovate and strengthen the AML framework. Of course, this is not to take away their individual innovations and stem competition, but rather, mutual cooperation within VASPs should be focused on enforcing AML standards at a regional level. Indeed, it is trite that end-users would have their own preference of VASPs which they engage with. However, to ensure there are no gaps within the regulatory firewall, these VASPs should operate harmoniously among themselves for matters such as end-user information disclosure, sharing of information pertaining 'blacklisted' individuals, as well as facilitating mutual strengthening of security functions. To that end, it is the regulatory bodies - central banks, larger financial institutions, and regulatory institutions - within these economies which have to facilitate such development. Else, it is unlikely that VASPs will take initiatives in this area, particularly where there is a general lack of incentive to do so after they fulfil the minimum obligations to comply with domestic law.

As a whole, these recommendations are intended to lay out a long-term sustainable framework to enhance AML measures within VASPs, and move towards an end-goal of the harmonisation of international trade law. However, to achieve such this, there is undoubtedly significantly more work that needs to be done, both at a domestic level, and a regional level. The first step towards achieving this aim however, seems to be to

[169] Anja Ipp, 'Regime interaction in investment arbitration: Climate law, international investment law and arbitration' (12 January 2022, Kluwer Arbitration Blog). <http://arbitrationblog.kluwerarbitration.com/2022/01/12/regime-interaction-in-investment-arbitration-climate-law-international-investment-law-and-arbitration/> accessed 30 November 2022.

[170] Efthymios Papastavridis, 'Interpretation of Security Council Resolutions under Chapter VII in the Aftermath of the Iraqi Crisis' (2007) 56(1) The International and Comparative Law Quarterly 83.

overcome the inertia, and begin a multi-faceted, multilateral dialogue in the realm of DDAs. Only through mutual cooperation and involvement of key stakeholders, tangible and effective change would arise.

To that end, perhaps lessons can be learnt from the European approach towards DDAs and VASPs. Under the recent Markets in Crypto-Assets Regulation ("MiCA") which is expected to come into force in February 2023.[171] As a regulation, the introduction of MiCA would create binding obligations on European Union ("EU") Member-States following its entry into force.[172] Very briefly, MiCA introduces a blanket definition to DDAs as "a digital expression of value or rights that can be transferred and stored electronically, using distributed registry technologies or similar technologies".[173] This harmonised taxonomy was established with consultation from the private sector (under the European Banking Authority") way back in 2019.[174] This taxonomy is hence undoubtedly to be applauded for this reason. The incorporation of private standards would allow for greater consideration of the nuances of DDAs such as the inclusion of "rights" within the definition. Further, while it must be noted that the use of a regulation as opposed to a directive signals a heavy-handed approach from this supranational organisation, perhaps such is required, given the transboundary nature of the asset and interconnectedness of Europe. In that regard, perhaps the economies of the Four Asian Tigers could look upon such a model to foster greater cooperation. More likely however, this would come at a later stage once these economies have a chance to properly consider the impact of MiCA following its enactment into EU legislation.

It must similarly be noted that MiCA is generally silent on AML provisions, with only a mere reference to the European Central Bank to handle all AML related legislation.[175] Additionally, the EU has not yet drafted a European-wide surveillance regime. The current position under the AMLD5 directive merely requires EU States to establish their own version of DDA-related AML provisions.[176] While this is rather unfortunate, many commentators note that with the introduction of MiCA and the overarching goal for harmonisation of DDA-related laws, a harmonised AML provision is only inevitable.[177] Nonetheless, for the Four Asian Tigers, what can be gleaned from this is that the harmonisation of AML provisions remains a long-term goal. Step-by-step harmonisation should first be considered before moving towards longer-term goals including AML

[171] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937' COM2020/593 final 24 September 2020.
[172] ibid 1.
[173] ibid 3.
[174] ibid 23.
[175] ibid 1.
[176] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for purposes of money laundering or terrorist financing, and amending directive 2013/36/EU [2018] OJ L 156/849.
[177] Koen Byttebier and Konstantinos Adamos 'Cryptoassets – a new frontier for money laundering and terrorist financing: legal changes to address the increasing AML risk' ahead-of-print [2022] Journal of Financial Crime <https://doi.org/10.1108/JFC-10-2022-0262> accessed 2 December 2022.

provisions. Undoubtedly, if the EU were to rush to harmonise through MiCA, this would be putting the cart before the horse - one would likely have to question whether its categorisation of what constitutes DDAs were truly effective in practice. Hence, perhaps it is due time that the Four Asian Tigers took the first step, and made the plunge into moving towards greater regional cooperation in this field.

5 Conclusion

Ultimately, DDAs present a novel financial technology, which has seen widespread adoption by both individuals within major and minor economies in recent times. However, as nations seek to take advantage of this new asset and out-position each other to attract investors, a disharmonious regulatory framework inevitably arises. Indeed, key culprits of this regulatory race include the four economic leaders in East Asia – Singapore, South Korea, HKSAR, and Chinese Taipei; also known as the Four Asian Tigers. Named after their and rags-to-riches story, each individual economy has had a history of embracing technological developments to get to where they are today. However, as they embark on the next step of their growth, each of these economies are vying to become world-class financial hubs within East Asia. To that end, they would inevitably have to address the controversial question of the particularly polarising financial instrument which has been gaining traction – that of DDAs.

In that regard, this paper sought to explore and take a snapshot of the current AML framework across thematic investigations into the regulatory framework of DDAs. In particular, it considers the position of these economies across three core issues within DDA regulation – their taxonomy and treatment of DDAs, rules and regulations surrounding custodians and service providers of these assets, and finally, their compliance and compatibility with international obligations, through the lens of AML laws and regulations. This area is particularly important given the current international climate and sanctions regime in place which DDAs seem to undermine; the lack of a central regulatory institution undoubtedly stroking much fear within both domestic and international policy makers. Unfortunately, despite the transboundary nature of these assets, there is clear disharmony both regionally across these economies, as well as under broader international law standards.

From the analysis conducted, one can identify that each of the economies seem to be taking a different thematic approach towards DDAs. Singapore seems to be the most stringent on matters pertaining to regulation, preferring to adopt a top-down, rather heavy-handed approach towards DDAs. Conversely, South Korea has taken the “minimum standards” approach, looking to strike a balance between maintaining the decentralised aspect of these assets, while setting up minimum core obligations for VASPs to follow, including the AML laws. HKSAR similarly embraces the technological developments under VASPs, urging stronger capacity building and information sharing measures and

encouraging cooperation within the private sector. Chinese Taipei however, has a rather new infrastructure surrounding DDAs, and the position of the legislative framework around DDAs has yet to be set.

These clear regulatory themes which these economies have adopted all find their grounding within the international legal framework set out by UNIDROIT and the FATF. What is particularly striking however, is that the domestic standards set out by these economies (with the exception of Chinese Taipei), seems to be more robust than the current taxonomy set out by UNIDROIT. In that regard, one can assume that international law would thus operate as a 'gap-filling' mechanism in the event that a new and novel instrument arises in the coming years. Similarly, the regulatory themes can all be found within the recommendations laid out by the FATF. Currently, HKSAR's framework is the most compatible with that of the FATF, particularly where the international task force has been looking to embrace evolving corporate standards of DDAs. Yet, while the HKSAR is best poised to take the lead in AML and regulatory compliance of DDAs, the high standards of regulations might not look the most attractive to investors and end-users. In that regard, a balance needs to be struck, drawing on the experiences of South Korea and Singapore, to further develop a harmonised framework in the region.

To that end, this paper makes two core suggestions in the realm of DDAs. First, an emphasis should be placed on the age-old doctrine of international comity, particularly within regulators. While competition among policy-makers across these regions undoubtedly spurs on regulatory innovation, and is beneficial to the overall standards surrounding DDAs, an emphasis should be placed on mutual cooperation towards a harmonised framework. This is especially the case where DDAs are known to operate in a transboundary manner. Mutual respect for the legislative systems within the region would set the ground for developing a unified taxonomy and regulations surrounding AML efforts within the region, removing the need for gap-filling mechanisms. Such similarly promotes regional cooperation, while strengthening the overall efforts of AML provisions. Secondly, this paper firmly believes that Chinese Taipei, South Korea and especially Singapore should follow the examples set out by HKSAR in embracing the rapid development of technologies, giving wider discretion towards VASPs. While, undoubtedly, top-down regulatory oversight on these institutions is required, it should come with a degree of trust that VASPs understand the market and are best positioned to address the wider policy concerns. In that regard, there is significant potential to allow and encourage VASPs to the table, both to provide their technical expertise on the matter, but similarly be allowed an opportunity to perhaps to accept the jurisdiction of international law in establishing an AML framework, while similarly enhancing the sanctions regime of the UNSC.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 2 - 1/2023