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.