Journal of Digital Economy Research. 2023. 1. P. 90–108
DOI 10.24833/14511791-2023-1-6-90-108

Received: 15 September 2022,
Revised 3 November 2022,
Accepted: 20 December 2022

FRAGMENTATION OF ARTIFICIAL INTELLIGENCE INTERNATIONAL REGULATION: CHALLENGES

by Alexey A. Sazhinov

Abstract. The issue of AI development and application is high on the international agenda now. One of the reasons is its excessive popularity among the public. Numerous international actors are now developing AI regulations. It is both universal and specialized international organisations with global and regional reach. Informal international fora are also active in this area. This process is a complex one and incorporate different factors which are both of objective and subjective character. In effect, AI regulation all the more often becomes a political tool for promoting economic interests of national IT companies or an instrument for secretariats of international organisations to keep a high profile. National AI regulation is often considered as a shield against malign use of AI by Western governments to manipulate domestic processes in other countries and to interfere into internal affairs. There are also different approaches which are practiced by intergovernmental organisations depending on their specialization. While specialized fora strive to build common grounds for the development and use of AI, regional organisations attach broader perspective to AI regulation and tend to politicize it. These various factors are likely to result in a fragmented regulatory field in this area according to national borders or borders of military and political alliances.

Keywords: Artificial intelligence, regulation, fragmentation, digital challenges

For citation: Sazhinov A. (2023) Fragmentation of Artificial intelligence international regulation: challenges. *Journal of Digital Economy Research,* vol. 1, no 1, pp. 90–108. (in English).
DOI 10.24833/14511791-2023-1-90-108

Information about the author:

Alexey Sazhinov – Independent researcher.
76, Prospect Vernadskogo Moscow, Russia, 119454
SazhinovAA@yandex.ru
ORCID: 0000-0002-5206-3113

Introduction

AI regulation is a broadly discussed topic at the moment. In fact both public authorities, regional and universal international organisations, academia, businesses, international NGO's are now dealing with AI related issues. Many countries have launched AI strategies and legislation on AI application in specific areas such as autonomous vehicles (CoE, 2022). International organisations initiate various binding and non-binding instruments. One of the examples is UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021). The European Union (EU, 2022) and the Council of Europe are in the process of developing their hard-law instruments. Large companies introduce ethical codes (Facebook*, Facebook's five pillars of Responsible AI). International NGO's take an active part in relevant activities at the national and international level within broadly promoted "multi-stakeholder approach". They are supported by their host-countries (primarily Western ones).

Reasons for such AI popularity are complex and unite both objective and subjective factors. Moreover, this process is highly politicized. AI has become an instrument for interference into domestic affairs. As a result, we are likely to see competing AI regulations in different regions. The development of a truly universal regulation is questionable in the near future.

Review

Research papers and articles on AI regulation mainly focus on the issue whether such regulation is needed and if so on its scope, shape and related risks while ignoring the analysis of existing developments in this area and their most probable results.

The researches usually consider that fragmented international regulation of artificial intelligence is the result of the lack of insight. However, usually this is not the case. The fragmentation appears to be an accepted risk in an attempt to develop such international regulation which would be friendly for national companies from particular countries.

The researches presuppose that the intentions of all international actors are benign and aim at developing AI regulation for the common good (see, for example, Erdélyi, Goldsmith, 2020). Another problem of existing research in the sphere of AI regulation is a widely spread assumption that this is an objective process (see, for instance, Stahl, Rodrigues, Santiago, Macnish, 2022). In fact, this is not the case. This appears to be a rather limited approach as international actors are usually guided by national interests in case of governments which may incorporate the interests of national largest companies. This is the reason why the US is rather cautious about international AI regulation. It would inevitably burden its largest IT giants. At the same time, the EU which IT industry is lagging behind the US one is so keen to regulate this sphere.

As artificial intelligence is broadly discussed both domestically and internationally, raising this issue is a way to attract attention to a particular international organization, NGO or an officer of an organisation. In practical terms, this means additional extrabudgetary contributions for specific projects.

The issue of fragmentation of AI regulation is touched upon in article "Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy" (Feijóo, Kwon, Bauer, Bohlin, 2020). However, this is considered as one of the risks rather than a mainstream and the most likely path of the development of AI regulation.

Discussion

This paper seeks to look on existing regulatory developments in this area and tries to analyze the effects of current tendencies in the sphere. At the moment we are witnessing a full-speed fragmentation of the international regulation of AI. There are some factors which presuppose this process.

First, this is an interest by Western countries to develop some AI rules in close circles in order to impose them lately on the rest of the world. In practical terms, this finds a reflection in Global Partnership on Artificial Intelligence which was established at the initiative of and effectively promotes the approaches which have been developed within OECD. The situation here is similar to that of the Convention on Cybercrime which was developed within the Council of Europe and is promoted as a "golden standard" in this sphere far outside the area of the Council of Europe.

Second, as mentioned previously, many international organisations, large NGO's, politicians seek to profit on the topic of artificial intelligence as it is broadly discussed now.

Third, it is a well-grounded perception by some governments that AI technologies are used by some states to interfere into domestic affairs of others. As a result there is a desire to establish national systems which would prevent such a use of artificial intelligence.

These factors are likely to be effective in a long term. Apparently, a number of blocks emerge united by common interests with regards of AI and they may create some hard-law legal frameworks for AI development and application. However, these would have a limited geographical scope.

AI regulation is discussed against the background of a global competition. It primarily unrolls between US and Chinese IT giants. We see a battle for billions-large revenues along with the number of users between large IT-companies. A platform's greater audience does not only mean greater income but also aggregated data which promises more efficient AI tools in the future. A wide spectrum of tools is used to win this competition. The US uses politicization of AI issues as one of them. This includes politically motivated PR campaigns and the adoption of politically motivated regulatory provisions which are aimed at barring competitors from new technologies

(The Guardian, Biden administration imposes sweeping tech restrictions on China, 2022). Thus, we see all the more subjective non-defined characteristics being attached to the AI. A democratic/responsible/ethical AI design/governance is one of them (EU, Intervention by President Charles Michel at the Summit for Democracy, 2021, GPAI, GPAI 2022 Ministers' Declaration, 2022, OECD, Tools for trustworthy AI a framework to compare implementation tools for trustworthy AI systems, 2019, OECD, OECD framework for the classification of AI systems, 2022).

Some international organisations propose that the use of AI in public domain implies special requirements for AI systems. For example, the Council of Europe in its Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law which were finalised in December 2021 (CoE, 2022) stated "in the context specificity of the risks posed by AI in the public sector in light of its specific role in society, such a transversal framework may be supplemented by additional legally binding or non-legally binding instruments at sectoral level". OECD considers public domain as a specific sphere of AI application as well (OECD, 2019) This approach would inevitably result in closing the market of public service AI solutions from the countries other than military and political allies.

AI is broadly used in moderation and prioritization of content in social media and search engines. Such systems were introduced by all the social media such as Facebook*, Instagram*, YouTube, Twitter and many others (Facebook*, How does Facebook use artificial intelligence to moderate content?). Moderation and prioritization sphere becomes all the more politicized. Large Western IT-companies demonstrate their readiness to apply biased and politically motivated moderation and prioritization techniques. For example, only this year YouTube has blocked accounts of some dozens Russian TV-channels including regional ones (Ministry of Foreign Affairs of the Russian Federation, Foreign reprisals against Russian journalists and media since the start of the special military operation to defend Donbass). Those social media which refrain from deleting pages of Russian media block them in specific countries.

Another example is the scandal that unrolled as a result of changes in Facebook* moderation techniques which allowed calls for violence against the Russians (Reuters, Facebook* allows war posts urging violence against Russian invaders, 2022). In fact, we see that some US internet companies become a long arm of their government. The main objective of such cooperation is to create a mechanism which would allow translating the narratives predefined by the authorities to the population of their own country as well as to that of other states. We witness all the more prolific use of social media, search machines etc. as foreign policy tools. Security services directly interfere into moderation and prioritization practices to promote governmental or private interests (BBC, Zuckerberg tells Rogan FBI warning prompted Biden laptop story censorship, 2022). Arab spring demonstrations which were ignited by social media tools showed a destructive potential of AI-driven content prioritization. AI prioritization due to its broad reach coupled with micro-targeting technologies allow reaching a large number of people with the messages which are most suitable for them.

So, IT companies turned into psychological operations' long arm. One of the most vocal and known tool applied in the hostilities which are gaining momentum in the international relations now is information. Weaponisation of this area through manipulative techniques effectively prevents reaching a common understanding on global AI regulation. This issue has been discussed in the UN for several years (see, for example report ITU, United Nations Activities on Artificial Intelligence (AI), 2022). Moreover, many AI technologies can be considered as double-purpose ones starting from various drones and ending AI tools to analyze satellite images.

This inevitably leads to the establishment of national and possibly regional regulations which would ensure information security of a country which would be aimed at minimizing potential use of foreign social networks to interfere into domestic affairs while promoting national ones. Consequently, governments which become targets of such psy ops strive to oppose them by promoting own internet companies and limiting activities of foreign ones including by regulatory means. Western social media are not permitted in China and Iran. These countries have developed their own services such as WeChat, Sina Weibo, Soroush, Cloob, Aparat.

We can assume that AI will play all the greater role in social media in the future. Ability to form large databases and to train AI thanks to them is another asset which business and governments are not likely to share as it means creating a better AI which is able to function in a concrete society with all its inherent features. This data may be considered as confidential. Since databases become more complex and detailed, they allow more precise predictions of societal behavior and reactions to different challenges. It looks as if this is one of the reasons for EU to demonstrate so much concern about personal data protection. This may also be a driving force for the US to make some concessions to the EU with this regard to resume a data transfer practice (EU, Questions & Answers: EU-U.S. Data Privacy Framework). Personal data is apparently considered as a strategic resources for AI advancement which is not to be shared with competing players.

In April 2021 the European Commission introduced its Proposal for a Regulation on artificial intelligence (EU, 2022). If adopted, it will constitute a hard-law regulation of AI. As declared in the document, its main rationale is the protection of human rights including personal data. Another noteworthy one is to prevent fragmentation of the European single market with regard to these solutions. Thus, the European Commission is aware of the risk of AI regulation fragmentation but is ready to overcome it at the regional level apparently hoping that it would be consequently possible to impose EU's regulatory approaches on the countries which export relevant AI solutions to the members of the European Union. A short-term goal is likely to control foreign IT companies in the European market as the EU companies are very sparely represented in the sphere of new communication technologies such as search engines, social networks and other internet solutions.

The Commission's proposal contains prohibition on use of social scoring systems, manipulation algorithms and indiscriminate facial recognition. A possible reason for these restrictions is lacking competence of EU companies in these spheres. Indeed, there is no social media from EU countries. The most known facial recognition Clearview AI is from the US. In the future this will give rise to different approaches to human rights application in digital sphere in global dimension. It is hard to imagine that the countries possess strong potential in these areas would prohibit relevant technologies

Largest IT-companies accompanied by specialised NGO's try to gain competitive advantages by wording international standards for different AI applications. There are numerous examples of such approach. For instance, there is a special platform for cooperation between digital companies and the Council of Europe. They are invited at the meetings of relevant Council of Europe committees which effectively develop international standards in digital area. It is also worth noting that relevant NGO's also take part in the meetings of competent Council of Europe bodies. International Telecommunication Union in its annual report (ITU, 2022) states that NGO's feature the majority of UN events on AI. This happens through various multi-stakeholder mechanisms which Western countries are actively lobbying. There is great risk that this is used to artificially outnumber the rest of the world by bringing in additional Western representatives and corrupt regulatory mechanisms in global international organisations. The latter may lose trust of non-Western global players. As a result we may see alternative forums and IT regulation platforms.

One more factor leading to fragmentation and regionalization of AI regulation is the western concept of a rules-based world order (Vylegzhanin, Nefedov, Voronin, Magomedova, Zotova, 2021). This concept implies that a group of developed states is trying to create their own rules for AI without proper consultations with the majority of the world. Further they are going to impose these rules on the rest of the world. This plan does not seem to be functional and efficient. Various Western organisations develop AI regulation of a general character. They are the European Union (EU, 2022), the Council of Europe (CoE, 2022), the Organisation for Economic Co-operation and Development (OECD, 2019) and some other informal alliances such as the Global Partnership on Artificial Intelligence.

Such approach demonstrates its inefficiency. It would inevitably result in unequal protection of persons in their relations with AI. In fact it may mean an appearance of such a regime when the data of the population in the developing countries would be misused and exploited by internet companies for the sake of better products for people in developed ones. Excluded countries which are large players in that market prefer to try to establish universal legislation in this area through UN system or other bodies in which they take part.

AI regulation fragmentation is to deepen further while IT play all the more important role in daily life and people spend more time in virtual reality which envisages for example the concept of metaverses. It appears that people will consume the bulk of information along with spending their money through metaverses' gateways in the

near future. This would result in more governmental control over this sphere. Effectively, the access to metaverses would be a matter of survival for many enterprises in B2C sphere. Barring a company from a metaverse would severely affect its sales. AI future legal regulation will be aimed at establishing a framework when access of some products and companies to domestic markets is limited due to national security considerations or economic reasons. It can be also expected that economic, military and political blocks would construct their own metaverses with own digital infrastructure.

Conclusion

The most real scenario for future AI regulation is fragmentation according to the borders of military and political alliances. We see that the EU intends to limit some AI applications as they allegedly contradict ethic values (EU, 2021). Thus, national and regional regulations are likely to bear an ideological component which would make difficult if impossible to bridge the differences in the future if a proposal to develop a global AI hard-law regulation of a general character is voiced.

When we are talking about universal AI regulation these differences may in fact only allow developing soft-law instruments of limited thematic scope covering some specific areas which deal with a limited quantity of personal data in areas which are in no way politicized. Several such tools are developed with the UN (ITU, 2022). For example, Project Domain of normative applied ethics at the intersection of AI and nuclear science, technology and applications, referred to as the Ethics of Nuclear and AI is developed within IAEA. ITU in cooperation with WHO works on a standardized assessment framework for the evaluation of AI-based methods for health, diagnosis, triage or treatment decisions, ITU also conducts standardization activities for services and applications enabled by AI systems in autonomous and assisted driving. UNECE tries to define technical requirements applied by the automotive sector worldwide (UNECE, 2019; UNECE, Automated driving UNECE is driving progress on Autonomous Vehicles).

* Facebook, Instagram and Meta are recognised as extremist organisations and are prohibited in the territory of the Russian Federation.

References

1. Council of Europe, AI initiatives – interactive map, electronic resource: https://www.coe.int/en/web/artificial-intelligence/national-initiatives, 2022

2. Recommendation on the Ethics of Artificial Intelligence https://unesdoc.unesco.org/ark:/48223/pf0000380455, 2021

3. Facebook's five pillars of Responsible AI https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/

4. Questions & Answers: EU-U.S. Data Privacy Framework https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

5. Biden administration imposes sweeping tech restrictions on China https://www.theguardian.com/us-news/2022/oct/07/biden-administration-tech-restrictions-china, 2022

6. United Nations Activities on Artificial Intelligence (AI) 2021 https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2021-PDF-E.pdf, 2022

7. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex-%3A52021PC0206, 2022

8. UNECE: driving progress on Autonomous Vehicles https://unece.org/DAM/trans/doc/2019/wp29grva/Autonomous_driving_UNECE.pdf, 2019

9. Automated driving UNECE is driving progress on Autonomous Vehicles https://unece.org/automated-driving

10. Hello, World: Artificial intelligence and its use in the public sector https://www.oecd-ilibrary.org/docserver/726fd39d-en.pdf?expires=1673561870&id=id&accname=guest&checksum=0DB9A8EF6610DDE66BCB9BFA125652C7, 2019

11. Tools for trustworthy AI a framework to compare implementation tools for trustworthy AI systems https://www.oecd-ilibrary.org/docserver/008232ec-en.pdf?expires=1673531426&id=id&accname=guest&checksum=B7CFD256835F222E44DFD7AEC2EB6D73, 2021

12. Recommendation of the OECD Council on Artificial Intelligence https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, 2019

13. OECD framework for the classification of AI systems https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf?expires=1673562225&id=id&accname=guest&checksum=EE3A09363130A18004BF7D3A7FA486FB, 2022

14. Regulating artificial intelligence: Proposal for a global solution https://www.researchgate.net/publication/341615195_Regulating_Artificial_Intelligence_Proposal_for_a_Global_Solution, 2020

15. A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values https://www.researchgate.net/publication/359194759_A_European_Agency_for_Artificial_Intelligence_Protecting_fundamental_rights_and_ethical_values, 2022

16. Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy https://www.researchgate.net/publication/341181427_Harnessing_artificial_intelligence_AI_to_increase_wellbeing_for_all_The_case_for_a_new_technology_diplomacy, 2020

17. GPAI 2022 Ministers' Declaration https://www.gpai.ai/events/tokyo-2022/ministerial-declaration/, 2022

18. Legitimacy of what?: a call for democratic

AI design https://www.hhai-conference.org/wp-content/uploads/2022/06/hhai-2022_paper_35.pdf, 2022

19. Chapter 8 of the National Security Commission on Artificial Intelligence's final report https://reports.nscai.gov/final-report/chapter-8/

20. Intervention by President Charles Michel at the Summit for Democracy https://www.consilium.europa.eu/en/press/press-releases/2021/12/10/intervention-by-president-charles-michel-at-the-summit-for-democracy/, 2021

21. Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on

human rights, democracy and the rule of law https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b, 2022

22. How does Facebook use artificial intelligence to moderate content? https://www.facebook.com/help/1584908458516247

23. Foreign reprisals against Russian journalists and media since the start of the special military operation to defend Donbass https://mid.ru/ru/press_service/journalist_help/repressions/?lang=en, 2022

24. Facebook allows war posts urging violence against Russian invaders https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/, 2022

25. Zuckerberg tells Rogan FBI warning prompted Biden laptop story censorship https://www.bbc.com/news/world-us-canada-62688532, 2022

26. Questions & Answers: EU-U.S. Data Privacy Framework https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

27. The concept "rules-based order" in international legal discourses https://www.mjil.ru/jour/article/viewFile/1190/1095, 2021