DOI: 10.17803/2313-5395.2021.3.17.403-422

European Artificial Intelligence Act: Should Russia Implement the Same?

Armen Zh. Stepanyan

Ministry of Economic Development of the Russian Federation, Moscow, Russia

Abstract: The proposal for a European Union Regulation establishing harmonized rules for artificial intelligence (Artificial Intelligence Act) is under consideration. The structure and features of the proposal of this regulatory legal act of the integrational organization are analyzed. EU AI Act scope is analyzed and shown as wider than the current Russian one. The act will contain harmonized rules for placing into market, operation and use of AI systems; bans on certain artificial intelligence methods; special requirements for AI systems with high level of risk and obligations of operators of such systems, harmonized transparency rules for AI systems designed for interaction with individuals, emotion recognition systems and biometric categorization systems, AI systems used to creating or managing images, audio or video content; market surveillance and supervision rules. The provisions of the Act, the features of the proposed institutions and norms, including extraterritoriality (as for GDPR before that raised many questions), risk-oriented approach (which is based both on self-certification and definite criteria for high-risk systems), object, scope, definitions are considered. The possible key concerns based on case-law to undermine possible discrimination are expressed. The author expresses conclusions about the advisability of (non) application of these institutions or rules in Russia.

Keywords: artificial intelligence; AI; artificial intelligence regulation; EU AI Act; EU AI Regulation

Acknowledgements: This study was supported by Russian Foundation of Basic Research (RFBR), research project 18-29-16172.

Cite as: Stepanyan, A.Zh., (2021). European Artificial Intelligence Act: Should Russia Implement the Same? *Kutafin Law Review*, 8(3), pp. 403–422, doi: 10.17803/2313-5395.2021.3.17.403-422.

Contents

I. Introduction

"*Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world. And* I r*eally would not want this monopoly to be concentrated in whose that specific hands, therefore, if we are leaders in this area, we will also share these technologies with the whole world, as we today are sharing atomic technologies, nuclear technologies"* Vladimir Putin said during the All-Russian Open Lesson, September 1st, 2017.[1]

More than a year has passed since the publication of the principles European Commission[2] wants to develop on the regulation of artificial intelligence (AI) systems and some comments on it (Stepanyan, 2020). Now, April 2021, the only European Union's legislative initiator, European Commission presents a proposal for European Union regulation establishing harmonized rules for artificial intelligence[3] (Artificial Intelligence Act, AI Act). In 2017, the European Council

[1] 'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day, *Russia Today* (Sept. 1, 2017). Available at: https://www.rt.com/news/401731-ai-rule-world-putin/ [Accessed 14.05.2021].

[2] European Commission, White Paper on Artificial Intelligence — A European approach to excellence and trust, COM(2020) 65 final, 2020. Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Accessed 14.05.2021].

[3] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021)206 final. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788 [Accessed 14.05.2021].

called for a "*sense of urgency to address emerging trends*" including "*issues such as artificial intelligence..., while at the same time ensuring a high level of data protection, digital rights and ethical standards.*"[4]

At the Commission supporting document, this Act is called the Regulation on the European Approach to AI. This style shows that while the Council of Europe's work on AI legal standards is progressing enough (at different levels[5] and in different Council of Europe bodies), the European Union claims itself to be the leader in AI regulation in Europe.

II. The Structure and Definitions in AI Regulation

Proposal supporting documents reveal that Commission will follow its own idea set you in White Paper to introduce complex AI regulation. This proposal is first step out of three. Second will be liability framework and third will be sectoral safety legislation revision.

The proposal of the AI Act is presented in 85 articles, 10 of them are devoted to amendments to the old legislation and 75 in 11 sections — directly to AI regulation. The proposal provides for a wide base of definitions, including the definition of an artificial intelligence system.[6] It refers to software that has been developed using one or more of the methods and approaches listed in Annex I to the Regulation and is capable, for a given set of human-defined goals, to generate results such as content, predictions, recommendations or decisions affecting the environment, which they interact with. Methods and approached are divided into 3 groups: (a) machine learning approaches, including supervised, unsupervised and reinforcement learning, (b) logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) statistical approaches, Bayesian estimation, search and optimization methods.

[4] European Council, European Council meeting (19 October 2017) — Conclusion EUCO 14/17, 2017, p. 8. Available at: https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf [Accessed 14.05.2021].

[5] All its activity showed at COE webpage https://www.coe.int/en/web/artificial-intelligence [Accessed 14.05.2021].

[6] Article 3 of the Proposal.

On the one hand, it is wider than the Russian definition of artificial intelligence set out in the National strategy for the development of artificial intelligence for the period until 2030, approved by the Presidential decree No 490 on October 10, 2019. According to this "*artificial intelligence is a set of technological solutions that allows to imitate human cognitive functions (including self-learning and search for solutions without a predetermined algorithm) and to obtain, when performing specific tasks, results comparable, at least, to the results of human intellectual activity. The complex of technological solutions includes information and communication infrastructure, software (including those that use machine learning methods), processes and services for data processing and finding solutions.*" EU definition covers all three groups but the Russian one covers directly only the first with machine learning and the second that is human cognitive, others indirectly by methods included in a set of technological solutions. On the other hand, the Russian definition covers not only software solutions (as a system) but also infrastructure (hardware), logical processes and services defining this "set."

Among other definitions, it is worth highlighting such subjective ones as "intended purpose," "reasonably foreseeable misuse," "significant change." Such wordings exist already in product safety regulations, Directive 2006/42/EC on machinery (Machinery Directive[7]). Wordings are inconsistent sometimes (Mazzini, 2019) and it will be logical if Commission will harmonize such wordings.

It seems that the use of such definitions in Russia should be supported by judicial practice or recommendations, or other soft law acts of the supervisory authorities or the legislator, and, accordingly, it is advisable not to use such or similar subjective (evaluative) definitions at the present time in the Russian Federation. The only big law in Russia at the field of digital technologies that uses risk-approach is the Personal Data Protection Law. There is no sufficient court and administrative practice on defects of risks devaluating models. Competent Russian body (Roscomnadzor) uses a more formal approach aimed to fine companies

[7] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), published at OJ L 157, 2006, p. 24.

despite its own recommendations that are very fragmentary and vague. Thus, changing this approach aiming to establish legal certainty will help Russia to build business and governmental (and therefore civil) environment where risk assessment is an understandable and common procedure. Assuming even under new AI Act possible aims of use, character and subjects of use require some shift in mind paradigm. We can predict that Russian authorities having political will can distribute more legal certainty by court and competent body's delegated acts and form new risk approach model of businesses and structure of public institutions. If there are no efforts about this, developers of AI systems will feel insecure or even afraid.

"Serious incident" is defined in AI Act as any incident that directly or indirectly leads, could lead or may lead to the death of a person or serious damage to his health, property or environment; or serious and irreversible disruption to the management and operation of critical infrastructure.

In Proposal supporting documents, EU uses some of the Council of Europe's AI glossary definitions: for example, algorithm is set as "*Finite suite of formal rules (logical operations, instructions) allowing obtaining a result from input elements. This suite can be the object of an automated execution process and rely on models designed through machine learning*." Current Russia's position towards the Council of Europe makes it impossible to believe that Russian authorities will accept that such an important definition will be not fixed statically in legislation but referenced from such a non-trusted politically integrational organization.

III. The Scope of Regulation

Article 1 of the Act as the object of regulation establishes harmonized rules for the commissioning, operation and use of AI systems, bans certain artificial intelligence methods, special requirements for AI systems with high level of risk and obligations of operators of such systems, harmonized rules of transparency for AI systems intended for interactions with individuals, emotion recognition and biometric categorization systems, AI systems used to create or manipulate images,

audio or video content; market surveillance and supervision rules. The software development process as such is excluded from the scope of regulation, however, during development, in fact, all the requirements of the AI Act on the use of AI systems must be considered. Developers as actors are excluded from the direct scope of the EU AI Regulation, which in fact can require introduction of special compliance titles or even departments. White paper mentioned that developers liability can be introduced. We will see if it will be included in final acts.

Harmonization is very important for EU as there is a risk that diverging national approaches will lead to market fragmentation and can create obstacles especially for smaller companies to enter multiple national markets and scale up across the EU Single Market. This is why Member States generally support a common European approach to AI. In a recent position paper[8] Member States recognize the risk of market fragmentation and emphasize that the "*main aim must be to create a common framework where trustworthy and human-centric AI goes hand in hand with innovation, economic growth and competitiveness*." This initiative is compliant with principles of subsidiarity and proportionality. In Russia, certainly, it should be governed at the federal level with no derogations at the regions.

The AI Act scope includes providers placing on the market or operating AI systems in the EU, regardless of whether these providers are registered in the EU or outside the EU, users of artificial intelligence systems located in the Union; providers and users of AI systems that are located in a third country, but the result of such a system is used in the EU. This scope of application of the AI Act is extraterritorial and imputation due to the fact that the developer and provider of the system cannot quite expect and foresee not even the customers themselves, but the application of the results of the systems by such customers. This situation is close to the imputation of jurisdiction and has roots in

[8] Non-paper — Innovative and trustworthy AI: two sides of the same coin, Position paper on behalf of Denmark, Belgium, the Czech Republic, Finland, France Estonia, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden, 2020. Available at: https://www.permanentrepresentations.nl/binaries/nlatio/documents/publications/2020/10/8/non-paper---innovative-and-trustworthy-ai/Non-paper+-+Innovative+and+trustworthy+AI+-+Two+side+of+the+same+coin.pdf [Accessed 14.05.2021].

similar provisions of the GDPR (General Data Protection Regulation), which have found its application in Russia. Obviously, this provision is aimed at ensuring that numerous US and China technology software companies, even when developing AI systems, are mindful of the EU requirements and may not enter the EU market with non-compliant AI systems. There are many issues regarding application of extraterritorial jurisdiction in more simple digital technologies domains, such as cloud computing (Sangwoo, 2018). It seems that for AI Act extraterritorial jurisdiction we will see the same big flow of questions as EDPS and national data protection bodies now see for GDPR extraterritorial jurisdiction.

As for the United States, it may seem that a new Biden presidency may see politically attractive for AI cooperation with EU. On some matters that is true. But some of them may become a taboo. For example, regarding the mentioned EU criteria for high-risk AI systems the United States might seek an arrangement with the EU that will allow companies located in the U.S. to self-certify as meeting them, subject to U.S. government control, under a system similar in concept to the Privacy Shield. Mutual recognition of conformity assessments also could be considered (Broadbent, 2021). This may help both win the geopolitical competition between China's illiberal model of AI regulation and democratic states' values-based model (Lawrence and Cordey, 2021). According to the former Google CEO Eric Schmidt "Europe will need to partner with the United States on these key platforms."[9] In late February, he estimated that China was only a few years behind the U.S. in developing artificial intelligence technologies but "Europe is not going to be successful doing its own third way" between China's state-led and the U.S. light-touch approaches.

AI systems intended for military purposes use, as well as bodies of third countries and international organizations, even if they fall under the scope of general scope rules of AI Act, but at the same time use such systems within the framework of agreements with the European Union or Member States on cooperation in the field of law enforcement and judicial authorities are excluded from the scope of the AI Act.

[9] Ex-Google chief: European tech 'not big enough' to compete with China alone. Politico. Available at: https://www.politico.eu/article/ex-google-chief-eric-schmidt-european-tech-not-big-enough-to-compete-with-china-alone/ [Accessed 13.05.2021].

IV. Rules and Regulations

The proposal of AI Act also defines bans on the use of certain AI systems and practices. Among the prohibited, for example, is the use of real-time biometric systems in public places. Still, there is an exclusion, among other things, for such a purpose: a targeted search for specific potential victims of crime, including missing children. In Russian Federation, regional and federal authorities are promoting the use of street cameras to search for missing children. However, unlike the proposal of AI Act, it does not indicate a ban on other uses. This absence should be treated as the absence of guarantees of non-violation of human rights such as right to privacy, right to biometric personal data protection etc.

It should be noted that the bans on the use of certain AI systems and practices itself constitute restrictions on the freedom to conduct business (Article 16 of EU Charter of Fundamental Rights ("the Charter")) and the freedom of art and science (Article 13) to ensure compliance with overriding reasons of public interest such as health, safety, consumer protection and the protection of other fundamental rights ("responsible innovation") when high-risk AI technology is developed and used. Those restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and likely infringements of fundamental rights.

The use of AI systems for social rating should be considered as a positive ban. "*Evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behavior or known or predicted personal or personality characteristics, with the social score leading to*" detrimental or unfavorable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behavior or its gravity is forbidden. China practice will be set as not allowed in EU.

But current wording proposal for Regulation as "*the detection, localization, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA*" expressly allows Member state police to use

facial recognition for after-the-fact identification of suspects, as the FBI did after the Capitol riot.

Moreover, the use of AI systems may lead to discriminatory outcomes. Algorithmic discrimination can arise for several reasons at many stages without any intent and it is often very difficult to detect and mitigate (here mentioned reasonably foreseeable misuse is not so foreseeable). Complications may arise due to imperfect architecture of application and creators who mechanically embed their own prejudices and labels when making the classification picks. People can misuse AI output the way that is not fit for the intended purpose in concrete cases. Furthermore, bias causes specific issues for AI methods dependent on input data, which might be unrepresentative, incomplete or contain historical biases that can strengthen existing inequalities with not real scientific and evidence-based legitimacy. Developers or users could also intentionally or unintentionally use proxies that correlate with protected characteristics under EU non-discrimination legislation such as race, sex, disability etc.[10] Although being based on seemingly neutral criteria, this may disproportionately affect certain protected groups giving rise to indirect discrimination (e.g., using proxies such as postal codes to account for ethnicity and race). The algorithms can also introduce themselves prejudices in their intellectual mechanisms by preferring certain characteristics of the data on which they have been trained. Differentiating levels of accuracy in the use of AI systems may also disproportionately affect certain groups, for example facial recognition systems that do not detect person as person those using wheelchairs.

Much more social consequences leading to formation of new forms of structural discrimination and social exclusion can be taken by society if other fundamental rights (e.g., right to education, social security and social assistance, good administration etc.) guaranteed by Charter will be violated in such domains as judiciary or law enforcement, public administration and employment. Currently at the EU market (same is true for Moscow and Saint-Petersburg being the main Russia cities)

[10] An example of such use of postal codes — ProKid (not in use anymore) to assess the risk of recidivism — future criminality — of children and young people in Amsterdam. These AI decisions were issued for a reasonable period of time despite postal codes are often proxies for ethic origin as ruled by the CJEU, Case C-83/14.

HR service in fact is assisted by AI technical solutions playing crucial role (more and more). Potential candidates in terms of discriminatory filtering at different moments of recruitment procedures or afterwards may be negatively affected. In social welfare domain there are cases where unemployed people were suspected of being discriminatory profiled by the administration of social welfare assistance. Financial institutions and other organizations might also use AI for assessing individual's creditworthiness to support decisions making influence onto access to credit and other services such as housing. In some cases it can be useful for people because their chances will be greater based on diverse data, but in some cases the risks of unintentionally induce biases for assessing scores exists, if not properly designed and validated. AI models trained with past data can be used in law enforcement and criminal justice to predict trends in the growth of lawbreaking in certain geographic areas, to recognize potential victims of crimes such as domestic violence or to evaluate the threats posed by individuals to commit offences based upon their criminal records and overall conduct. Both at the borders of EU for asylum seekers and migrants and inside the territory of Union for these categories and citizens risks of discriminatory decisions of predictive AI policing systems exists.

In case such discrimination occurs an affected person almost has no means to collect evidence. Moreover, if they want to have some judicial or administrative remedy, they do not know that they had been affected by an AI system. They have no tools to prove it. Even for administrative or court authorities it may be very difficult to distinguish between discrimination reasons and discrimination itself (Wachter, Mittelstadt and Russell, 2021). This means lack of transparency for both parties. The guaranteed right to be heard as well as the right to an effective remedy and fair trial cannot be realized. The same thing exists with the presumption of innocence that is hampered by opacity of some AI judicial software. This can lead to obstacles for persons charged with a crime to defend themselves and challenge the evidence used against them. At the end, if this software give motivation to public authorities not in addition but instead of themselves then the latter may not be able to reason their decisions and right for good administration will be violated (Wachter, Mittelstadt and Russell, 2021).

AI Act uses risk-oriented approach that was supported explicitly during public consultation. Blanket approach was not considered a better option. Risks are also planned considering the impact on rights and safety and the types of risks and threats should be based on a sector-by-sector and case-by-case approach. This permits to have flexible mechanisms that allow it to be dynamically enabled as the new concerning situations emerge, abuses adapt and technology evolves.

High-risk systems got the rules for their classification, which, of course, should be recognized as a good mean of legal certainty. For personal data, these criteria were issued in the Russian Federation in competent bodies delegated acts long after the adoption of the federal law, which did not contribute to legal certainty and respect for human rights. All high-risk AI systems for EU must have a system for managing risk, quality, tracked logic for selecting data streams, transparency, and the provision of information to users. The proposal contains a sufficient number of requirements for high-risk AI systems, one of the mandatory requirements for such systems is the ability to review the operation of such systems by human individuals. The retention period for system logs should be based on national law or user agreement.

Commission foresees that compliance with these specific requirements and obligations would imply costs amounting to approximately 6,000 euros to 7,000 euros for the supply of an average high-risk AI system of around 170,000 euros. Approximate costs for human oversight for AI users are estimated to be 5,000 euros to 8,000 euros per year. Verification costs could amount to another 3,000 euros to 7,500 euros for suppliers of high-risk AI.

AI Act involves liability rules. Existing EU product certification system includes bodies and authorized representatives as legislative institutions for the market. For example, as at the market of medical devices — the sector of goods that directly affects the health and life of people, and, therefore, these are high-risk goods — every manufacturer of AI system from outside the European Union will be obliged to appoint an authorized representative in the EU. Thus, having jurisdiction over at least the representative, the EU uses them partly as "hostages" of the fulfillment of the requirements of EU legislation by foreign providers. The requirements in the proposal of AI Act set out for importers,

and even for distributors of AI systems. Just like at the medical device market, institutions of notification and evaluation bodies are being introduced. Notification bodies are used to maintain registers of AI systems, evaluation bodies — to assess the compliance of these systems with legal requirements. Such existing conformity assessment system has been operating for a long time not only in relation to the medical devices products, but also for many other sectoral areas of conformity assessment (children's toys, chemical materials, etc.). AI act will establish requirements for both types of institutions, as well as conformity assessment procedures, certificates for marking with the CE mark (common for current conformity assessment in the EU). We should have in mind that the Cybersecurity Act[11] sets up voluntary cybersecurity certification framework for Information and communications technology (ICT) products, services and processes while the relevant Union product safety legislation sets up mandatory requirements.

High-risk AI systems will be listed in special database established to storage EU-wide database for stand-alone high-risk AI systems with mainly fundamental rights implications (Article 60) to facilitate the monitoring work of the Commission and national authorities. The database will be operated by the Commission and provided with data by the providers of the AI systems, who will be required to register their systems before placing them on the market.

For all non-high risk AI systems, AI Regulation would not impose any obligations or boundaries except for some minimal transparency responsibilities in two specific cases where people might be deceived which are not effectively addressed by existing legislation. This would include: obligation to inform people when interacting with an AI system (chatbot) in cases where individuals might believe that they are interacting with another human being; label deep fakes except when these are used for legitimate purposes such as to exercise freedom of expression and subject to appropriate safeguards for third parties' rights.

[11] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 07.06.2019, pp. 15–69.

Expected in 2022 as a second step in a complex three-step AI regulation liability framework Product Liability Directive review will possibly harmonize some parts of civil liability (which is now under national law). It will include solution with regard to liability for damages/harm caused by AI systems and effective compensation for victim claims. Liability rules will cover post-effects for AI systems including possible damage and its compensation while AI Act rules will protect against possible violations of fundamental rights and safety. Both steps will cover *ex-ante*, ex-post effects, however, liability reform will adapt liability rules compliant with foundational concepts (e.g., the definition of AI), and legal obligations with regard of operations of economic operators set by the AI Regulation. AI issues are close to robotics issues and Commission has intention to adapt traditional offline market of machinery to emerging risks and technologies. Proposal for new Machinery Regulation also issued in April 2021 emphasizes importance of both new laws: AI and Machinery acts. In October 2020 European Parliament already expressed their recommendations according to which European Commission should base new legislation on the liability rules. Its position[12] presents full text of proposal for new Regulation on liability for the operation of AI systems. As this resolution was issued before new proposals of AI Act and Machinery Regulations from European Commission, it is obvious that Commission should elaborate some minimum on technical issues such as wordings and terms.

It is worthwhile to evaluate positively the rules on the transparency of algorithms in some AI systems and on the very fact of interaction with the AI system, on the possibility of Member States to "open" regulatory sandboxes (which is very important for some innovative areas, such as unmanned vehicles (Stepanyan, 2019)).

The transparency responsibilities restrict the right to protection of intellectual property (Article 17(2) of Charter), but proportionally since they will be limited only to the minimum necessary information

[12] Civil liability regime for artificial intelligence. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)) Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf [Accessed 14.05.2021].

for individuals to exercise their right to an effective remedy and to the required transparency during supervision and enforcement. Current EU legislation, including Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure binds with confidentiality and non-disclosure any public authorities and notified bodies if they should have access to confidential information or source code to examine compliance.

UK was one of the first creators of regulatory sandboxes inside EU: children rights and freedoms online was key area that ICO asked expressions of interests for and approved some of the projects in 2019 (ICO 2021). France had the very strict feature for its sandboxes: all projects were not exempt from the scope and rules of GDPR (General Data Protection Regulation) so it permitted to build all data flows in compliance with law at all stages even during prototyping.

Digital technologies regulatory sandboxes were enacted in Russia in 2021. One of the projects in unmanned vehicles by Yandex. According to this context Russia is one of first countries outside EU that have such regime in digital field and already have big AI project in one of the sandboxes. Norway implemented half-France, half-UK model sandbox (Datatilsynet, 2020): GDPR (and fundamental rights and ethics) rules cannot be exempted but during development stage no enforcement will be applied to participant in case of non-compliance.

Title V of Proposal clearly sets strict rules on Member States for derogation from EU data protection rules: Member States should apply their supervising and control powers to such AI regulatory sandbox. Moreover, "*Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place*" (Article 53 (3) of Proposal). Such strict insisting on GDPR application shows that GDPR is long-term institution at EU market and all businesses and public bodies should learn how build privacy-by-design compliant systems as there is no markers GDPR will be deprecated.

To guide the above, the EU intends to establish a European Artificial Intelligence Board (EAIB). This Board will be composed of representatives from national AI authorities as well as the European Data Protection Supervisor. In my opinion, this body appears to be based more on the structure of BEREC (European Regulatory Authority for Electronic Communications) rather than EDPS (European Supervisory Authority for Data Protection). But as for competence (Article 58 of Proposal) the Board will ease a smooth, effective and harmonized implementation of this regulation by contributing to the effective cooperation of the national supervisory authorities and the Commission and providing advice and expertise to the Commission. It will also collect and share expertise and best practices among Member States and contribute to uniform administrative practices, including for the functioning of here mentioned regulatory sandboxes. Furthermore, it will issue opinions, recommendations or written contributions on matters related to the implementation of this Act.

At national level, Member States will have to designate one or more national competent authorities and, among them, the national supervisory authority in order to supervise the application and implementation of the regulation. The European Data Protection Supervisor will act as the competent authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of AI Act both for the latter and GDPR.

Title VIII sets out the monitoring and reporting obligations for providers of AI systems for the post-market monitoring in case there is AI-related serious incidents and malfunctioning (Article 62). Market surveillance authorities would also control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market. Market surveillance and control of AI systems in the Union market as per Regulation (EU) 2019/1020 shall apply to AI systems covered by AI Act. The market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access, any data or documentation. Moreover, where necessary to assess the conformity of the high-risk AI system with

the requirements for such systems and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system (Article 64). They will also monitor compliance of operators with their relevant obligations under the act. Member States will appoint some existing bodies with the powers to monitor and enforce as it does not foresee creation of any additional bodies or authorities at Member State level. It does not touch existing system and allocation of powers of ex-post enforcement of obligations regarding fundamental rights in the Member States. When necessary for their mandate, existing supervision and enforcement authorities will also have the power to request and access any documentation maintained following this regulation and, where needed, request market surveillance authorities to organize testing of the high-risk AI system through technical means.

Framework for the creation of codes of conduct is set in Article 69. Such codes of conduct boost providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems. But providers of non-high-risk AI systems may create and implement the codes of conduct themselves. Those codes may include voluntary obligations, for example concerning accessibility for persons with disability. Such self- regulation will help to boost groups of providers be more compliant or more specific. For Russia it can be useful for special economic zones — innovation centers — to introduce such code of conducts for its residents — tech companies. It will permit to have more qualified developers and responsible software projects and companies.

The obligation to respect confidentiality of all information and data, including intellectual property, received during all relations for implementation of Act set out (Article 70). This provision is very practical and should be inherited in Russian legislation.

Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of AI Act and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. Fines are up to 30 million euros or up to 6 % of the annual world turnover, which will be higher. For institutions and bodies of the Union, the fines are lower — up to 500 thousand

euros. GDPR has enacted a similar system (big absolute and turnover fines) that seems to be successive in terms of market surveillance.

We can estimate the same approach from national bodies of EU Member States. Some of them are not issuing fines, some do. For example, French court uphold the decision of CNIL (French data protection body) to fine Google Inc. (which is a US company operating Google search and Gmail mail services) for 50 million euros[13] (it is a big sum but much lower than its 4 % of turnover, which is approximately 3.2 billion euros). It is considered the biggest fine now. LfD of Lower Saxony in Germany fined notebooksbilliger.de AG (online e-commerce portal and retail chain dedicated to selling laptops and other IT supplies) for more than 10 million euros for constant video surveillance and recording storage for 60 days.[14] This sum is sufficient for the company that is not as big as Google. Thus, applying to small AI developers' companies such big fines may make them bankrupt. Administrative fines for violation of the GDPR are higher than fines for violations of the Russian legislation on personal data, but Russia provides for a wider range of sanctions, which may lead to more serious penalties (up to and including imprisonment). Statistics of imprisonment as a measure for violating Article 137 of the Criminal Code of the Russian Federation show that there are five cases in both 2020 and 2019 and it is not possible to delimit cases that clearly rely on infractions of personal data requirements and privacy overall. So we can see that the main liability is administrative and civil, despite civil is very low (Dmitrik, 2020).[15]

The difference is that GDPR applies to a wider range of companies processing personal data, but to a very narrow range of companies selling AI systems. Many of them are able to have AI Act compliance lawyers or developers.

[13] € 50 million fine for Google confirmed by French Court. Available at: https://noyb.eu/en/eu50-million-fine-google-confirmed-conseil-detat. It is remarkable the CEO of NGO submitted the claim to CNIL is Max Schrems, famous by his ECJ cases Schrems I and Schrems II. [Accessed 14.05.2021].

[14] GDPR: German laptop retailer fined € 10.4m for video-monitoring employees. Available at: https://www.zdnet.com/article/gdpr-german-laptop-retailer-fined-eur10-4m-for-video-monitoring-employees/ [Accessed 14.05.2021].

[15] Average compensation for personal data leaks for example in first half of 2018 in Russia was only 800 rubles (which is approximately 9–20 euros in different years).

Once adopted AI Act will come into force in default term — 20 days after its publication in the Official Journal. Entry in force is scheduled in 24 months after that date, but some provisions will apply earlier. 24 months is long enough period for Member States to choose and set up their national bodies but tech companies may elaborate some act provisions overtaking solutions, mainly by technological measures. The risk exists that before they even apply some provisions, those will require correction or adaptation to some technologies despite its technology-neutral character.

Year 2012 EU bundle of telecom legislation was fit for giving boost to EU economy because of mainly net and technology neutrality what covered both offline telecommunications infrastructures rise and real new technology software and means such as Skype (true EU economical miracle of 2010s). And it worked. Now with mainly US players on EU market it is not possible to answer exactly, will such players follow the rules of the game or pull the fifth ace out of their sleeve.

V. Conclusion

As can be seen from the above, the proposal of AI Act is not simple and small and is quite complex being only one part of overall EU AI regulation. An AI system as object of regulation receives a status that is similar to the status of a high-risk or even possibly dangerous product or service with its own specifics. Classification of AI systems helps to both developers and users to know their rights and freedoms.

Some rules are set to be easily fit and integrated into the EU legal system, but are not suitable for other countries due to the lack of specific features of the EU legal system in such countries. This statement can be fair also for Russia.

It is worthwhile to further explore the applicability and impact assessment report in order to talk about the possible use of a particular institution in Russia. It is necessary to make many changes in legislation and law enforcement practice in order to be able to adopt a similar comprehensive act and use its achievements. However, the question on the expediency of such complex changes exists, and the answer to this question is not so obvious. At the moment if the legislator is willing to

introduce AI legislation reform in Russia, the possibility of proposing the introduction and implementation of individual rules looks for us much more successful and applicable, while the principles document — the Concept for the development of regulation of relations in the field of artificial intelligence and robotics technologies until 2024 — already exists in Russia. In my view, Russia should continue work on this topic and in short-term perspective (1–3 years) this field can be ready for Russia AI Act.

References

1. Broadbent, M., (2021). *What's Ahead for a Cooperative Regulatory Agenda on Artificial Intelligence?* Center for Strategic and International Studies (CSIS). Available at: http://www.jstor.org/stable/resrep30085 [Accessed 14.05.2021].

2. Datatilsynet, (2020). *Regulatory Sandbox*. Available at:https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ [Accessed 14.05.2021].

3. Dmitrik, N.A., (2020). History, essence and prospects of personal data protection. *Vestnik grazhdanskogo prava* [*Civil Law Review*], 20(3), pp. 43–82, doi: 10.24031/1992-2043-2020-20-3-43-82 (In Russ., abstract in Eng.).

4. ICO. Information Commissioner's Office, (2021). *Regulatory Sandbox*. Available at: https://ico.org.uk/for-organisations/regulatory-sandbox/ [Accessed 14.05.2021].

5. Lawrence, C. and Cordey, S., (2020). *The Case for Increased Transatlantic Cooperation on Artificial Intelligence*. Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2020. Available at: https://www.belfercenter.org/publication/case-increased-transatlantic-cooperation-artificial-intelligence [Accessed 14.05.2021].

6. Mazzini, G., (2019). A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law. In: A. De Franceschi — R. Schulze (eds.), *Digital Revolution — New challenges for Law*. Available at: https://ssrn.com/abstract=3369266 [Accessed 14.05.2021].

7. Sangwoo, L., (2018). *A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing*. 539 p. Available at: http://dx.doi.org/10.2139/ssrn.3442428 [Accessed 14.05.2021].

8. Stepanyan, A.Zh., (2019). Problems of Regulation of Unmanned Vehicles. *Courier of Kutafin Moscow State Law University (MSAL)*, 4, pp. 169–174, doi: https://doi.org/10.17803/2311-5998.2019.56.4.169-174 (In Russ., abstract in Eng.).

9. Stepanyan, A.Zh., (2020). Digital Regulation: Digitalization or Humanization? *Courier of Kutafin Moscow State Law University (MSAL)*, 4, pp. 114–120, doi: https://doi.org/10.17803/2311-5998.2020.68.4.114-120 (In Russ., abstract in Eng.).

10. Wachter, S., Mittelstadt, B. and Russell, C., (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law and Security Review*, 41, doi: 10.1016/j.clsr.2021.105567.

Information about the Author

Armen Zh. Stepanyan, Cand. Sci. (Law), Task Force Co-Chairman, Ministry of Economic Development of the Russian Federation, Moscow, Russia
10 build. 2 Presnenskaya naberezhnaya, Moscow 125039, Russia
armen@stepanyan.com