ИНСТИТУТ
ЭКОНОМИЧЕСКОЙ
ПОЛИТИКИ
имени Е.Т. ГАЙДАРА

International Best Practice Analysis Department

Monitoring of international legal regulation trends aimed at development of legislation in the digital economy in Russia

Excluding risks in the use of AI in law enforcement, protection of intellectual property rights in training generative AI

Monitoring No.5 (May 2024)

Monitoring was produced by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Ivan Ermokhin, Researcher, International Best Practices Analysis Department, Gaidar Institute.
O. Magomedova, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Tatiana Malinina, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute

JUNE 10, 2024

"Great, true deeds are always simple and humble"

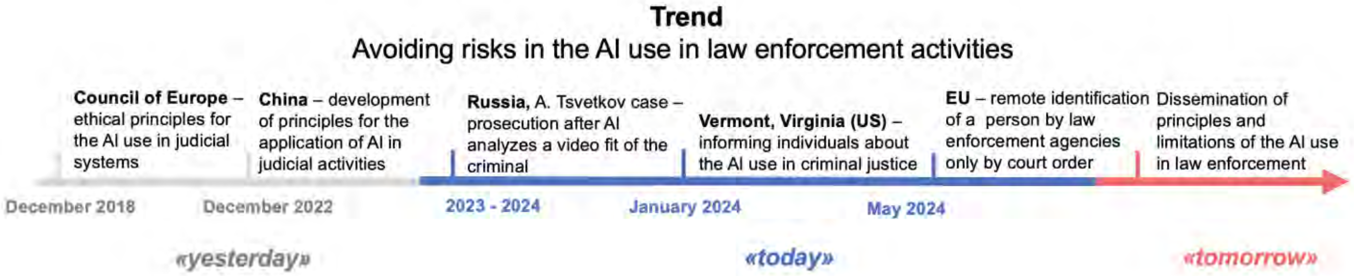
Leo Tolstoy

In May 2024, we can identify 2 events that define trends in the development of regulation of the digital economy.

Trend No. 1. Avoiding risks in the AI use in law enforcement activities

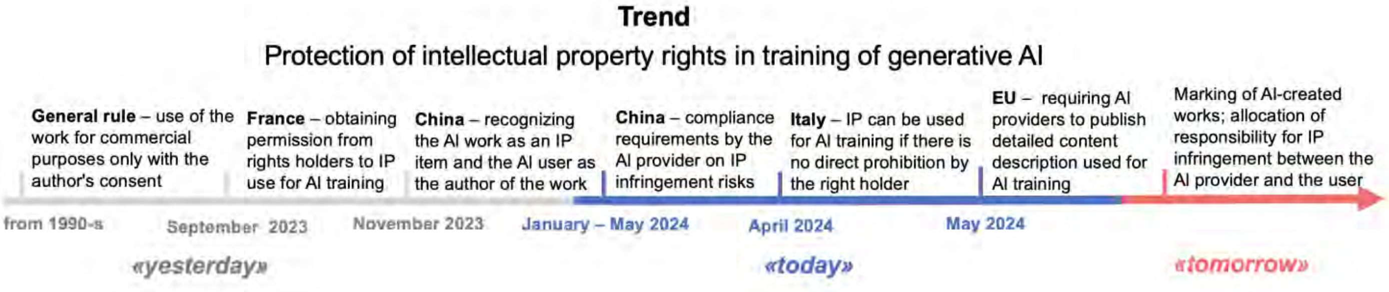
In Russia, the high-profile criminal case against Alexander Tsvetkov, heard in 2023-2024, demonstrated risks that may arise from the application of artificial intelligence (AI) in law enforcement. There is no special regulation in this area, and the instructions of the Ministry of Internal Affairs concerning the use of such technologies are classified.

In May 2024, the EU passed a law that classifies artificial intelligence used in law enforcement as high-risk, including allowing its use with court authorization for real-time biometric identification of suspects in public places. In addition, AI systems for criminal proceedings are also categorized as high-risk by US state bills. Back in 2018, the Council of Europe adopted basic provisions for the AI use in judicial activities: AI cannot replace judges, participants must be informed about its use, and data for AI training must be obtained from legal sources and processed in an understandable manner. Similar provisions were adopted in 2022 by the Supreme Court of China.


Trend
Avoiding risks in the AI use in law enforcement activities
Council of Europe – ethical principles for the AI use in judicial systems
China – development of principles for the application of AI in judicial activities
Russia, A. Tsvetkov case – prosecution after AI analyzes a video fit of the criminal
Vermont, Virginia (US) – informing individuals about the AI use in criminal justice
EU – remote identification of a person by law enforcement agencies only by court order
Dissemination of principles and limitations of the AI use in law enforcement
December 2018
December 2022
2023 - 2024
January 2024
May 2024
«yesterday»
«today»
«tomorrow»

Trend No. 2. Protection of intellectual property rights in training of generative AI

In May 2024, China published draft Basic Requirements for Generative AI Security, laying down requirements for its operators on measures to curb intellectual property rights (IPR) infringement. For example, if the dataset on which the AI is trained contains literary, artistic and scientific works, the provider is obliged to conduct a check for IP rights infringement in the content generated by the AI. The adoption of these rules is prompted by court cases in 2023-2024. For example, the Ultraman case to prohibit the use of content for training and for generating AI without the authorization of rights holders. A similar approach in the EU and France, which require service providers to implement a "sufficiently detailed summary" model - disclosure of IP used for content generation and AI training.


Trend
Protection of intellectual property rights in training of generative AI
General rule – use of the work for commercial purposes only with the author's consent
France – obtaining permission from rights holders to IP use for AI training
China – recognizing the AI work as an IP item and the AI user as the author of the work
China – compliance requirements by the AI provider on IP infringement risks
Italy – IP can be used for AI training if there is no direct prohibition by the right holder
EU – requiring AI providers to publish detailed content description used for AI training
Marking of AI-created works; allocation of responsibility for IP infringement between the AI provider and the user
from 1990-s
September 2023
November 2023
January – May 2024
April 2024
May 2024
«yesterday»
«today»
«tomorrow»

Key aspects

1. Avoiding risks in the AI use in law enforcement activities

The European experience

In law enforcement, AI has been used in the EU since at least the mid-2010s, including for surveillance in public places during certain events (e.g., the G20 summit in Hamburg).[1] The limits of such interference with people's rights have raised concerns, including among MEPs.[2]

In May 2024, the **EU** passed the AI Act,[3] which legitimizes the possibility for already constant surveillance in real time and in any public space of more than 6,000 people who are wanted on a European warrant for crimes.

The Act classifies a number of AI systems used in law enforcement activities as **"high-risk"**, which implies **increased requirements** for such systems: to ensure automatic recording of events throughout the life cycle of an AI system; to apply a risk management system, including testing, etc. The Act also provides for the use of a risk management system, including testing, etc.

For example, the use of remote biometric identification of suspects in real time in public places (tracking by AI on surveillance cameras) is prohibited in law enforcement activities but is allowed with the prior authorization of a judicial body for some particularly dangerous crimes (terrorism, human trafficking, drug trafficking, etc.). The list of crimes is quite broad.

Law enforcement profiling of individuals in criminal investigations is also allowed, but human oversight of AI is required.

Thus, the AI use in criminal investigations is possible in the EU subject to certain requirements for high-risk AI systems. Thus, the Law recognizes the risks of discrimination and violation of fundamental rights in the use of AI systems (e.g., safety - not to fear arrest just because an AI camera on the street signaled a match with a criminal). To mitigate such risks, the Law introduces requirements for high-risk AI - data quality, risk analysis, human monitoring of work and decisions, and the ability to fine-tune AI systems.

Whether compliance with these requirements will be sufficient to avoid creating distortions is questionable. For example, if the system is trained even on representative data showing that, for example, thefts are committed by people from the same country or of the same gender, then risks of discrimination are created - the AI system, trained on such data, may point to these people as suspects in the first place.

The EU has attempted to balance the risks and benefits of AI by imposing special requirements on high-risk AI for law enforcement.[4] However, Austria, for example, considers these measures insufficient to guarantee the rights of citizens; in its opinion, law enforcement officers are given too much power.[5]

It is worth noting that in 2018, the **Council of Europe**[6] developed and adopted ethical principles for the AI use in judicial systems,[7] which formed the basis for the regulation of this area in the EU. In particular, the list of principles includes requirements for the quality and security of systems, user awareness, and others.

The US experience

In the US, there is no AI regulation in law enforcement. This creates problems for the police in respecting the rights of suspects and complicates their defense, for example, in 2020, a man was arrested on suspicion of theft because facial recognition technology showed

[1] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

[2] https://www.patrick-breyer.de/en/ai-act-threatens-to-make-facial-surveillance-commonplace-in-europe/.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_24_2024_INIT.

[4] Decisions based solely on automated processing of personal data for the prevention and investigation of crime or the execution of criminal sanctions, except where safeguards for human controller intervention are provided, were previously prohibited by the EU Directive 2016/680 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680).

[5] https://data.consilium.europa.eu/doc/document/ST-9645-2024-ADD-1-REV-1/X/pdf.

[6] Council of Europe – ian international organization outside the EU structure.

[7] https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment.

he matched a photo of a criminal, but he did not commit theft.[8]

Vermont[9] and Virginia[10] bills (January 2024), categorize AI systems that significantly impact access to criminal justice as high risk. This means there are special requirements for risk management and for the data on which the AI is trained.

The approach of these states differs from that of the EU on two main issues:

1) It is not prohibited to the AI use, for example, to assess a person's risk of committing crime based on profiling alone.

2) No human oversight of AI is required, but it is required that those subject to AI-based decision-making be necessarily briefed on the use of such a system and its purpose, and, in Vermont, the way it works.

As a result, the transparency of AI systems, which affects the suspects' right to protection, is ensured by general requirements for high-risk AI (on the quality of the data used, risk management) as well as the suspect's right to obtain information about the operation of the AI.

China’s experience

There is no specific regulation of the AI use in law enforcement. However, in 2022, China's Supreme Court issued similar principles to the Council of Europe on the AI use in judicial activities.[11] At the same time, China has laid down special principles such as:

- AI should not substitute for a judge in making decisions.
- The responsibility for the decision lies with the decision maker, not the AI.
- The right of the user (judge, defendant, etc.) to reject AI products when making judgments.

Russia’s experience

There is no special regulation of the AI use in criminal proceedings in Russia. At the same time, among the main functions of the Ministry of Internal Affairs of Russia is the task of introducing AI into the information and analytical system,[12] however, there are no methodological recommendations on the use of these services in the public domain. The closed nature of such information makes it difficult to analyze and challenge decisions made using AI in the Ministry of Internal Affairs system, including the defense of suspects and defendants in criminal cases.

In 2023, a person was charged with murders based on the neural network's decision that he resembled the sketch of the criminal by 55% (the case against Alexander Tsvetkov) . Cases, the circumstances of the prosecution of which are like the case of Alexander Tsvetkov, are not available in open sources, but in the context of inaccessibility of data on the AI use in the system of the Ministry of Internal Affairs, this may mean the absence of not such cases, but their publicity. Taking into account the existing nature of the judicial and legal system (election of preventive measures, low proportion of acquittals), this aggravates the risks of prosecution of innocent people, and leads to the dilution of responsibility for the decisions taken during the investigation. The possibility of bringing charges because of a procedure with a non-transparent AI mechanism makes it difficult to establish who is responsible for the prosecution and defense of the accused.

It is possible in Russia:

1. Establish requirements for AI systems intended for use in crime investigation regarding the data used, including for training and testing, risk management, transparency, human control.

2. Provide legal guarantees that a decision generated with AI input cannot be made without human assistance. On the one hand, this means that a human is ultimately responsible for any decision, while on the other hand, holding them accountable is a matter of law enforcement.

2. Protecting intellectual property rights in generative AI training

Generative AI allows new content (text, computer code, images, audio and video) to be created in response to a user's request. The

[8] https://www.techpolicy.press/senators-explore-ai-in-criminal-investigations-and-prosecutions

[9] https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf.

[10] https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1.

[11] https://www.court.gov.cn/fabu/xiangqing/382461.html.

[12] Clause 12.62 of the order dated June 15, 2021, No. 444.

training of such AI often takes place on open data, which may contain IP-protected objects. This runs the risk of creating works that are like the copyrighted works of other authors.

Therefore, in May 2024, China and the EU adopted the first IP enforcement rules for generative AI training, which was prompted by a number of court cases where rights holders filed complaints about AI training based on their works without their authorization.

The experience of China

In May 2024, China released a draft "Basic Requirements for Generative AI Security".[13] **Generative AI service providers should**:

1) Designate a person responsible for the observance of IP rights when using IP by the system and in the generated content.

2) Have an IP enforcement strategy, including a list of risks of IP infringement.

3) In case of IP infringement not to use infringing datasets for AI training, conduct infringement verification.

4) Provide a mechanism for users to complain to the vendor about AI rights infringements by generative AI.

Regarding the need to obtain permission from copyright holders for the content used for AI training, in February 2024, a court in Guangzhou held the owner of a website that provided a content generation service for money liable. The court found that the system operated in such a way that, at the user's request, an image was created that was confusingly similar to the plaintiff's intellectual property. The court's practice shows **that AI that allows a user to make a request to generate content that involves copying IP or its individual elements will be treated as an infringement of IP law**. In this case, the general rule on the prohibit on commercial use of IP without a **license from the rights holder** applies.[14]

At the same time, a court in China recognizes an AI user's copyright on AI-generated works. In November 2023, a Beijing court ruled on a copyright infringement case involving an image created using Stable Diffusion. The AI-generated images are "works" under copyright law because they belong to the field of literature, art, are original and represent the result of human intellectual activity. The author is recognized as the plaintiff, who entered a query of keywords (type of image, depicted object, environment and style) and further adjusted the query. The court ruled out the authorship of the developers of the AI system on the generated image.

The experience of EU, France, and Italy

Ita Adopted in May 2024, the EU AI Act establishes the obligation of generative AI providers to:

1) Implement compliance with copyright law (e.g., check the data used by AI for protected IP objects).

2) Publish a detailed **description (summary) of the content** used to train the AI model (part 1 of Article 53), e.g. listing the main datasets, including an indication of major private or publicly available databases or archives. It is planned to develop a form for such a summary.

In the EU, there is a right for research organizations and cultural heritage institutions to the IP use without the permission of the right holders for scientific purposes. Similar to Article 23 of the Copyright Law of China.[15]

Among the EU countries, in September 2023, **France was the first** to introduce Bill No. 1630[16] on mandatory obtaining the consent of right holders when using IP objects for AI systems, including training of generative AI systems. **Without author's authorization**, it is possible to use only for **non-commercial** purposes. This reduces the risks of unlawful commercial use of IP objects while preserving the possibility of free use of such objects for socially useful purposes.

If a work is generated by an AI "without direct human intervention", the right holders are the authors or right holders of the works that made the generation of the work possible (Art. 2). However, it remains unclear how the specific

[13] https://www.tc260.org.cn/upload/2024-03-01/1709282398070082466.pdf

[14] Ст. 23 Закона об авторских правах https://www.most.gov.cn/ztzl/gjkxjsjldh/jldh2017/jldh17xgwj/201801/t20180104_137482.html

[15] П.14 Преамбулы Директивы ЕС № 2019/790 об авторском праве.

[16] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi

works that became the basis for the generation should be defined, how should the copyright on the work generated by the AI be assigned?

The French bill proposes to introduce collective management of AI-generated works through collective management organizations (to collect royalties). The draft law does not solve the issue of using for training works whose authors could not be identified. Such a proposal carries the risks of misidentifying the authors of the work, infringing the authors' rights to the name and to remuneration for the use of their works.

France also proposes to make it compulsory to mark that a work has been generated by an AI system - a similar rule has been introduced in **Italy's** draft AI law (April 2024). A sign or marking with the abbreviation “IA” (intelligenza artificiale) must be used.[17] Regarding the use of protected IP for AI training, Italy, unlike the EU and France, has offered a different approach - the right to freely use legally accessible data for training AI systems, unless such use is expressly prohibited by the right holders.

The US experience

No specific regulation has been enacted in the US. As a rule, the doctrine of “fair use” of copyrighted data applies - it is possible to use IP objects without a license in the circumstances defined:

1) Purpose (e.g., educational).

2) The nature of the use (non-commercial). This does not mean that every non-commercial use is recognized as bona fide and every commercial use as non-bona fide. For example, a “transformative use” (adding something new) would probably be considered fair use. Using a combination of image and text to train an AI is essentially “transformative” over the original data, which is theoretically recognized as fair use.

3) The character of the data itself: the greater the creative element, the lower the chances of fair use being recognized.

4) The amount of source data used.

5) The impact on the market and value of the protected data - whether unlicensed use harms the existing market (e.g. by displacing sales of the original) or the future market (the original will become less popular).

In 2023, lawsuits were filed in the US by US writers against OpenAI for using their texts for ChatGPT training and copying works without permission; a lawsuit by artists against Stability AI, Deviantart and Midjourney for unauthorized use of copyrighted images for AI training to produce more works of the same type without the consent of the original image authors. The complaints have been accepted for review, but rulings have not yet been given.

Russia’s experience

There is no regulation of IP for AI training in Russia.

However, it is possible to apply Article 1274 of the Civil Code of the Russian Federation - the right to use the publicized work or its part without the consent of the right holder and without payment of remuneration for informational, educational or cultural purposes. It is required to specify the name of the author and the source. That is, if the above conditions are met, the use of IP objects may be qualified as quoting, and IP objects may be used for training generative AI for commercial purposes, which entails infringement of IP right holders.

Thus, it is possible to highlight 3 approaches of countries to the use of data for AI training:

1) Requirement for AI service providers to comply to protect IP and publish information on data used for AI training (EU, France and China). In addition, generally, it is required to obtain authorization from right holders for commercial use of IP, without authorization - only for non-commercial purposes.

Courts in China and a bill in France propose to extend a general rule on obtaining authorization from right holders for commercial use of IP for AI training.

2) No special requirements for AI operators (US) while allowing bona fide use of IP for AI training without a license.

3) Free use of AI without the right holders' authorization, except for an explicit prohibit on use by the right holder (Italy).

The Russian approach to the right to use works for training AI without authorization is

[17] https://www.senato.it/service/PDF/PDFServer/DF/437373.pdf

similar to the EU and French approaches. Russia has no mechanisms to protect right holders from unauthorized use of IP objects for training generative AI systems.

To create such mechanisms, it is possible to supplement Part 4 of the Civil Code of the Russian Federation with norms:

- The right of the author/right holder to forbid the use of the work for training AI systems / algorithms.
- Marking of works created using AI/algorithms.