

LEGAL GUARANTEES OF OBSERVANCE OF INFORMATION RIGHTS OF INDIVIDUALS IN THE APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES BY COURTS: EUROPEAN EXPERIENCE AND PROPOSALS FOR UKRAINE

Oleh Zaiarnyi

Doctor of Law, Professor, Professor at the Department for Intellectual Property and Information Law, Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ORCID ID: 0000-0003-4549-7201

Abstract. The paper examines the system of guarantees of compliance with the information rights of individuals who are plaintiffs or defendants in litigation when using artificial intelligence during the trial of specific cases provided for by the legislation of the European Union. The study analyzes the relationship between the requirements for the development and application of artificial intelligence technologies provided for by the Regulation of the European Union "On Artificial Intelligence", as well as international acts of "soft law" with the content of positive and negative obligations of the Member States of the European Union to ensure guarantees of compliance with certain categories of information rights in the administration of justice.

The purpose of this work is to study the experience of the European Union and its Member States on the legislative consolidation and practical implementation of guarantees of observance of the information rights of individuals, participants in the judicial process, the formation on this basis of certain recommendations for improving the procedural legislation of Ukraine on relevant issues.

To achieve this goal, general and special methods of scientific knowledge were used in the study, such as dialectical, logical, analysis and synthesis, comparative law, and others.

The paper proves the connection between the principles of ethical and lawful use of artificial intelligence in the administration of justice, provided for by the legislation of the European Union, with the content of guarantees of fundamental information rights. In particular, we are talking about the right to non-interference in private and family life, to the confidentiality of information about individual forensic evidence, to protection from automatic court decisions, to access information about algorithms for making procedural decisions, to ensure personal cybersecurity, and others. The author proves that the guarantees of information rights of participants in a judicial process in which artificial intelligence is used can acquire a practical essence only if they are properly enshrined in law and must be observed during the trial of specific court cases. Also, the scientific opinion is substantiated, according to which the effective implementation of guarantees of information rights of participants in the judicial process is possible provided that a balance is ensured between the design of safe artificial intelligence technologies

controlled by decision-making judges and the conscientious, transparent and impartial use of such technologies.

In the conclusions, based on the results of the study, the main directions of adaptation of the legislation of Ukraine to the legislation of the European Union on the regulation of compliance with the guarantees of information rights of individuals participating in litigation in cases of the use of artificial intelligence technologies are identified. Along with this, separate recommendations have been developed to improve the procedure for using artificial intelligence technologies by the courts of Ukraine in judicial and administrative-procedural activities. A legal and technological model for implementing guarantees of information rights of participants in litigation in developing individual digital modules based on artificial intelligence is also proposed.

Keywords: European Union legislation; information rights; Justice; artificial intelligence technologies; a participant in the litigation; an individual.

The statement of the problem. The implementation of judicial and legal reform in various Member States of the European Union (hereinafter referred to as the EU Member States) is traditionally accompanied by the implementation of a set of measures aimed at the systemic digital transformation of the judicial process, strengthening the guarantees of citizens' access to impartial, fair and timely justice.

Artificial intelligence is recognized as one of the technological means of achieving these goals in many EU Member States (Zaiarnyi, 2021, p. 34).

Despite the advantages this technology brings to participants in various categories of disputes, the use of artificial intelligence in the administration of justice is accompanied by certain legal risks. These are, in particular:

- imperfection of data sets (including court decisions) used to train artificial intelligence. It is explained by the emergence of new social relations or circumstances, relevant changes in judicial practice, as well as the presence of discriminatory beliefs on the Internet;
- inaccessibility of algorithms to support court decision-making and the inability to establish the exact sequence of actions of the system and the motives for forming the appropriate conclusion. This causes risks of interference by third parties in the operation of algorithms for illegal purposes;
- threats to the privacy of persons applying to the court. Judicial information contains a lot of personal data, including sensitive data. There may be shortcomings in the functioning of modules responsible for the depersonalization of documents and, accordingly, violations of human rights to privacy. In addition, a potential threat is the destruction or misdirection of electronic data carriers;
- threats to the confidentiality of information. Leakage of information constituting professional, official secrets, etc., as well as information created or received in the course of proceedings;
- violation of the right to a fair trial. It is necessary to provide an effective mechanism of technical support to the population in case of shortcomings in the operation of the system, mandatory human control of decisions made by artificial

intelligence, and the ability to appeal and/or correct decisions (Report Reforming the Judicial System of Ukraine, 2020).

The analysis of these and other risks of introducing artificial intelligence in the litigation of various disputes indicates that most of them negatively impact the information rights of individuals participating in these disputes. First of all, we are talking about the right to confidentiality and security of personal data processing, to the prohibition of further processing of personal data, to the protection of data from automated processing, to the confidentiality of information set out in court case materials, to access to information about the results of the case, etc.

In order to ensure the necessary balance between the advantages of introducing artificial intelligence technologies into the procedures for resolving litigation with the participation of citizens and ensuring the fair use of this technology, the problem of developing a legal mechanism for observing the information rights of citizens participating in the judicial process is becoming of considerable relevance.

The purpose of this work is to study the experience of the European Union and its Member States on the legislative consolidation and practical implementation of guarantees of observance of the information rights of individuals, participants in the legal process, the formation on this basis of individual recommendations for improving the procedural legislation of Ukraine on relevant issues.

Research methods and materials. During the study, the method of analysis and synthesis was used to identify general trends in the use of artificial intelligence technologies in the administration of justice and to identify special patterns of violation of the information rights of individuals, which may manifest themselves as a result of the illegal use of artificial intelligence by judges or officials of the court apparatus, or other participants in court proceedings; Dialectical method for identifying the risks of illegal use of artificial intelligence technologies in the administration of justice, identifying trends in the development of these risks into violations of the information rights of individuals participating in the judicial process; comparative legal method in order to determine special legislative requirements for the use of artificial intelligence technologies in the administration of justice in certain EU Member States, to clarify the content of guarantees of information rights of individuals to whom artificial intelligence is applied in the administration of justice; logical method was used to determine the features of the structure and content of the legislation of individual EU Member States to clarify the legal, technological and ethical features of observance of the information rights of participants in the litigation when using artificial intelligence technologies.

To achieve the defined goal of the study, the author used the legislation of the EU, individual EU Member States, in particular Estonia, Spain, the Netherlands, and France, case law materials, and analytical materials summarizing the practice of using artificial intelligence in the trial of certain categories of cases.

Findings. To date, artificial intelligence technologies in most EU Member States, where they are used for the administration of justice, have been legalized as separate modules or functional subsystems of national judicial systems. Such EU

member states as Estonia, Spain, the Netherlands, France, Sweden, and others have directly approached the legislative consolidation of the legal possibility of using artificial intelligence technologies in the justice field.

These states have already adopted certain amendments to procedural legislation aimed at solving the problems of using artificial intelligence in the administration of justice.

At the same time, in these states, technical specifications for creating separate modules of national judicial systems based on artificial intelligence were developed and approved (Report Reforming the Judicial System of Ukraine, 2020).

Every 2 years, CEPEJ conducts a survey on the use of information technologies in the courts of the member states of the Council of Europe and divides these states into three groups depending on the intensity and effectiveness of their use of information technologies in courts since 2004. The data collected are published in the form of reports in which CEPEJ classifies information technologies according to their functions in the judicial process:

- direct support for judges and employees (office work, work planning, communication, database formation, support for work in the courtroom);
- support for interaction between the court and the parties (internal and external communication, except for videoconferencing, messaging, blogs, wikis, and the Internet) (Zaplotynskyi B., 2020).

Artificial intelligence at the current stage of development belongs to both groups of technologies, as it can serve as a means of proper support for the activities of judges and court employees, in particular, in the automated distribution of cases, the formation of judicial statistics, etc., and as a form of interaction between the court and a person, for example, with the help of chatbots.

Analysis of court decisions, particularly for predicting decisions, summarizing judicial practice, and maintaining judicial statistics.

Estonia has implemented a digital solution into the national judicial information and telecommunication system at the level of a separate module (subsystem) that automatically analyzes the submitted documents and provides recommendations on the draft court decision that the court can make based on the evidence submitted. The judge has the ability to review and approve or modify this decision, providing professional control over the process. This information resource also provides support in the search and analysis of the European Court of Human Rights practice and national judicial practice that corresponds to the presumption of dispute and the jurisdiction of litigation (sud.ua, 2023).

In Spain, artificial intelligence technologies are primarily integrated into the national judicial information and telecommunication system. The main purpose of artificial intelligence in the mentioned state is to support court decision-making, ensure the automated distribution of court cases, and analyze the case law of the European Court of Human Rights and the European Court of Justice.

In France, one of the clearest examples of information systems designed to integrate artificial intelligence technologies into the administration of justice is Predictive. It is a digital operating platform that provides access to more than 26

million legal documents, including court decisions and legislative texts. Using artificial intelligence algorithms, predictive allows lawyers to assess the likelihood of a positive resolution of specific disputes and predict possible amounts of compensation for damage or losses by court decision. To simplify the search for the necessary information or use other functions of the mentioned information resource, users can send requests in simple colloquial language, which helps to increase the relevance of search results (predictice.com, 2024).

Case Law Analytics is a tool that uses AI and mathematical modeling to assess litigation risks. It simulates the possible outcomes of court procedures in various areas of law, helping lawyers develop effective strategies and find relevant case law (lexisnexis.com, 2024).

At the same time, in France, judges complained about the violation of their rights due to the fact that court decisions were used to analyze the behavior model of a particular judge. Amendments were adopted to the legislation on the introduction of criminal liability for the analysis of judicial practice, making it possible to predict a judge's decision in a case.

In contrast to the above examples of the use of artificial intelligence in the judicial systems of individual Member States of the European Union, in the Netherlands, the practice of using this technology for pre-trial settlement of various categories of disputes is widespread.

E-Court is a private initiative in the Netherlands that offers online dispute resolution. The platform provides information on alternative dispute resolution and access to mediators and arbitrators through ADRPartners. The main goal of e-Court is to make justice more accessible and faster, reducing the cost and duration of traditional litigation (ecourt.co.nl, 2024).

Although the UK is not currently a member state of the European Union, its experience in the application of artificial intelligence technologies in certain areas of the court's activities is of considerable interest. In the mentioned state, artificial intelligence technologies are also used to generate an automatic electronic draft of a local court decision in civil cases, administrative offenses, and criminal offenses. The "Electronic Judge" system is fully functioning in the UK in the courts of first instance in cases in which the subject of dispute does not exceed 500 (five hundred) pounds sterling.

In England and Wales, on December 12, 2023, the Artificial Intelligence (AI) Guidance for Judicial Office Holders, designed to assist judicial officials in using artificial intelligence, was published.

It outlines the main risks and challenges associated with using AI, some suggestions for minimizing them, and provides examples of potential uses. Any use of artificial intelligence by or on behalf of the judiciary must comply with the main duty of the judiciary – to protect integrity in the administration of justice.

In the manual, potentially useful tasks include:

- artificial intelligence tools are able to summarize large amounts of text (as with any other resume, care must be taken to ensure that it is accurate);
- AI tools can be used to write presentations, for example, to suggest topics to cover;

- Administrative tasks, such as creating emails and memoranda, can be performed using artificial intelligence.

Tasks that are not recommended to be performed with the help of artificial intelligence include:

- legal research: AI tools are a bad way to conduct research to find new information that you can't verify yourself; they can be useful as a way of reminding you of material that you think is correct;

- legal analysis: modern public chatbots with artificial intelligence do not provide convincing analysis or argumentation (Vasyl Krot, Igor Golubovskiy, 2024).

The UK's experience can be particularly useful for Ukrainian courts. Automatic generation of an electronic draft decision based on uniform approved templates of procedural documents will allow you to pay more attention to the essence of the decision rather than its execution and prevent gaps and mechanical errors in court documents. At the same time, there are risks of recognizing this practice as violating the principle of independence of judges. Given the functional features of artificial intelligence, this principle should be applied to the content of the decision and not to the form of its adoption, which can be established by legislation at the national level.

The practice of introducing artificial intelligence in the use of artificial intelligence in foreign judicial systems: minimizing the procedural actions of the judge (court employees), speeding up the terms of the trial of the case, reducing corruption risks in the court's activities, simplifying technical procedures for analyzing legislation and judicial practice, calculating the amount of damage caused or caused losses, the possibility of preliminary calculation of the amount of monetary punishment, clarification and systematization of the motives by which was guided by the judge when making a decision on the case (Report Reforming the Judicial System of Ukraine, 2020).

For the EU and its Member States, the main legislative act that comprehensively regulates the use of artificial intelligence technologies in various spheres of public life, in particular in the administration of justice, is Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 establishing harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168 /2013, (EU) 2018/858, (EU) 2018/1139, (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Law) (Regulation (EU) 2024/1689, 2024) (hereinafter referred to as the EU Artificial Intelligence Regulation), which entered into force on August 1, 2024.

According to the EU Artificial Intelligence Regulation, EU member states have until August 2, 2025, to designate national competent authorities to monitor the application of rules for AI-based systems and carry out market surveillance activities.

This mandatory norm also applies to the highest authorities of the EU Member States, which are responsible for the digitalization of procedural rules for resolving various categories of disputes.

The preparation for the adoption of the EU Regulation on Artificial Intelligence and the development of unified approaches to the regulation of the use of artificial intelligence were comprehensive and based on a number of advisory acts adopted by the governing institutions of the EU, including: Resolution of the European Parliament with recommendations of the Commission on civil law on robotics 2015/2103 (INL) (European Parliament resolution, 2017), Communication of the European Commission to the European Parliament, European Council, Council of the European Economic and Social Committee and the Committee of the Regions "Artificial Intelligence for Europe" (European Commission, 2018), Recommendations of the High-Level Expert Group on Artificial Intelligence on Ethics for Trustworthy Artificial Intelligence (AI HLEG, 2019), Recommendation of the Committee of Ministers of the Council of Europe Cm/rec (2020)1 to Member States on the impact of algorithmic systems on human rights (Recommendation of the Committee of Ministers of the Council of Europe Cm/rec (2020)), "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust" (European Commission, 2020), European Commission Report on the Security and Liability Implications of Artificial Intelligence, Internet of Things and Robotics (European Commission, 2020).

Considering the potential risks and possible negative impacts of using artificial intelligence in guaranteeing and ensuring fundamental human rights and ethical standards, all these documents contain proposals for their compliance. In particular, the European Parliament Resolution 2015/2103 (INL) became the basis for introducing uniform legal standards and developing specific legal instruments for using artificial intelligence in the EU. It provides for the principles of strict compliance with the legislation on protecting personal data and ways to overcome the problems of human dependence on technical devices. The Recommendations of the High-Level Expert Group on Artificial Intelligence on Ethics for Trustworthy Artificial Intelligence also define the basic principles of its use: human-centric, i.e., artificial intelligence technologies should be developed, used, and monitored, ensuring compliance with fundamental human rights and ethical norms. "Robust AI" requires algorithms to be legitimate, secure, trustworthy, and resilient enough to handle errors or inconsistencies at all stages of the AI technology cycle. The recommendations contain 7 key requirements that artificial intelligence technologies must meet in order to be considered reliable: 1) human rights and oversight; 2) technical reliability and safety; 3) confidentiality and data management; 4) transparency; 5) diversity, non-discrimination and fairness; 6) social and environmental well-being; 7) accountability. The Recommendation of the Committee of Ministers of the Council of Europe Cm/rec(2020)1 to Member States on the impact of algorithmic systems on human rights contains obligations of states to protect and promote human rights and fundamental freedoms in the context of algorithmic systems.

Based on these developments, the provisions of the EU Regulation on Artificial Intelligence establish uniform obligations for operators of this technology and guarantee equal protection of the public interest and the rights of individuals

throughout the internal market on the basis of Article 114 of the Treaty on the Functioning of the EU.

On December 3, 2018, the European Commission for the Efficiency of Justice (CEPEJ) under the Council of Europe adopted the European Charter on the Ethical Application of Artificial Intelligence in Judicial Systems and the Justice Environment (Council of Europe, 2018). This document is the first international soft law act defining the ethical principles for using artificial intelligence in judicial systems.

The Charter emphasizes that the use of artificial intelligence technologies in judicial systems must comply with the guarantees of fundamental rights proclaimed in the Convention for the Protection of Human Rights and Fundamental Freedoms, other acts of the Council of Europe, in particular, Convention No. 108 "On the Protection of Natural Persons with regard to Automated Processing of Personal Data" and additional protocols to it. First, we are talking about the right to a fair trial, non-interference in personal and family life, access to information, etc.

One of the key principles of the Charter provides for ensuring equal treatment of all participants in the judicial process. The use of artificial intelligence algorithms should exclude prejudice or discrimination on the basis of race, gender, nationality, age, or other characteristics.

The charter also requires AI algorithms to be highly quality, reliable, and based on objective data. This ensures that court decisions that use AI technologies remain legal, reasonable, and predictable.

Along with the above, based on the principle of intelligibility, the use of artificial intelligence technologies should be transparent, and algorithms should be understandable to users, including judges, lawyers, and parties to cases. This ensures the right of the parties to know how decisions are made, which may affect their cases.

At the same time, the use of artificial intelligence technologies in the administration of justice should be based on the principles of control of the participants in the trial, on whose expression of will-specific procedural actions depends. Artificial intelligence cannot replace a person's final judgment. The Charter stipulates that artificial intelligence must remain under the control of a competent specialist, particularly a judge, who is responsible for the decisions made (Council of Europe, 2018).

However, the Charter states that its principles are advisory in nature. This means that the effectiveness of ensuring human rights depends on the practical implementation of these principles in the national judicial systems of the member states of the Council of Europe.

After the adoption of the EU Regulation on Artificial Intelligence on March 13, 2024, many EU Member States, in particular Estonia, Denmark, Finland, France, Germany, and Sweden, began extensive consultations on further law-making steps on the possibility of using artificial intelligence in the administration of justice. The starting points of such consultations are the classification of artificial intelligence in the field of justice as a high-risk technology, the impossibility of its application to assess the behavioral characteristics of participants in the judicial process, the

prohibition of assessing the activities of judges through intellectual profiling of the judge's work, and the strict observance of fundamental human rights.

The legal basis for such consultations is, in particular, the provisions of Article 5 of the EU Artificial Intelligence Regulation, which stipulate that prohibited AI practices that may violate fundamental human rights and ethical norms are: 1) placing on the market, commissioning or using an artificial intelligence system that uses subconscious, intentionally manipulative or deceptive methods of influencing the consciousness of an individual in order to significantly distort their behavior or the behavior of a group of persons by significantly distorting their behavior or the behavior of a group of persons by significantly distorting the behavior of a person. deterioration of the ability to make an informed decision, thereby prompting a decision to be made that a person/group of persons would not otherwise have made, in a way that causes or is reasonably likely to cause significant harm to that person, another person or group of persons; 2) placing on the market, commissioning or using an artificial intelligence system that exploits any vulnerability of an individual or a certain group of persons due to their age, disability or specific social or economic situation, with the aim of significantly distorting their behavior, which as a result causes or is reasonably likely to cause significant harm to these persons; 3) placing on the market, commissioning or using artificial intelligence systems to evaluate or classify natural persons or groups of persons over a period of time based on their social behavior or known, assumed or foreseeable personal or personal characteristics, with a social indicator resulting in one or both of the following: harmful or unfavorable treatment of certain individuals or groups of persons in social contexts, that are not related to the contexts in which the data was originally created or collected; harmful or unfavorable treatment of individuals or groups of persons that is unjustified or disproportionate to their social behavior or its severity; 4) placing on the market, putting into operation for this specific purpose or using an artificial intelligence system to assess the risks of natural persons for the purpose of assessing or predicting the risk of a criminal offense by a natural person solely on the basis of profiling a natural person or on the assessment of his/her personal qualities and characteristics (this prohibition does not apply to artificial intelligence systems used to support a human assessment of a person's involvement in criminal activity, that is already based on objective verifiable facts directly related to criminal activity); 5) placing on the market, commissioning for this specific purpose or using artificial intelligence systems that create or expand facial recognition databases through the non-targeted collection of facial images from the Internet or CCTV camera recordings; 6) placing on the market, commissioning for this specific purpose or using artificial intelligence systems to determine the emotions of an individual in the workplace and in educational institutions, except when the use of such a system is justified by medical or safety considerations; 7) placing on the market, commissioning, or using biometric categorization systems that classify individuals based on their biometric data to infer their race, political views, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation (this prohibition does not apply to any labeling or filtering

of lawfully obtained biometric data sets, such as images, based on biometric data, or the categorization of biometric data in the field of law enforcement); 8) the use of remote biometric identification systems "in real time" in publicly accessible places for the purposes of law enforcement agencies, unless such use is strictly necessary for one of the following purposes: targeted search for specific victims of kidnapping, trafficking in human beings or sexual exploitation, as well as the search for missing persons; prevention of a specific, significant and immediate threat to the life or physical safety of natural persons or a real or realistically foreseeable threat of a terrorist attack; locating or identifying a person suspected of having committed a criminal offence for the purpose of conducting a criminal investigation or prosecuting or executing criminal penalties for offences referred to in Annex II to the EU Artificial Intelligence Regulation, punishable in the Member State concerned by imprisonment or detention for a maximum term of at least four years.

Thus, the approach laid down in the norms of the EU Regulation "On Artificial Intelligence" regarding the information rights of individuals when using artificial intelligence technologies is manifested in the fact that they cannot create more significant risks to a person's private and family life, information security, access to fair justice, compared to the traditional way of their own behavior.

At the same time, due to introducing a system of specific restrictions on the use of artificial intelligence, the EU Regulation "On Artificial Intelligence" clarified the system of guarantees of information rights proclaimed in acts of the European Parliament.

By their content, they are aimed at limiting the illegal use of artificial intelligence for the purposes of profiling participants in court proceedings, conducting an automated assessment of their procedural actions, excessive interference in private and family life, preventing risks to the cybersecurity of users of electronic services in the field of justice, ensuring secure digital identification during court proceedings.

The legislative consolidation of this approach to setting the limits of the lawful use of artificial intelligence, in particular, in the field of justice, reveals the content of the positive and negative obligations of the EU Member States, defined for them by acts of the European Parliament and the EU Commission.

On December 15, 2022, the EU adopted the European Declaration on European Digital Rights (Declaration on European Digital Rights, 2022). According to its objectives, this EU soft law act demonstrates the EU's commitment to developing a safe and sustainable digital transformation based on the principle of human-centeredness and respect for human rights and freedoms. The above-mentioned Declaration develops the provisions of Digital Europe 2030, particularly in the context of using artificial intelligence technologies for justice purposes. Among the safeguards established by said document and that extend to the justice sector, the following can be mentioned:

Freedom of choice. People should benefit from a fair online environment, be protected from illegal and harmful content, and be empowered when interacting with emerging technologies like artificial intelligence.

Safety and protection. The digital environment must be safe. All users, from children to the elderly, should be empowered and protected from unlawful interference with family privacy when implementing national, local, and corporate digital solutions.

In the context of the formation of a system of guarantees for the observance of the information rights of natural persons participating in litigation, Regulation 2019/881 of the European Parliament and of the Council of April 17, 2019, on the European Union Agency for Cybersecurity (ENISA) and on the certification of cybersecurity of information and communication technologies, as well as the repeal of Regulation (EU) 526/2013 (the Cybersecurity Act) (hereinafter referred to as Regulation 2019/881) (EU Regulation 2019/881, 2019) is of great importance.

Unlike the acts of EU legislation on cybersecurity, which were adopted by the European Parliament until 2018, Regulation 2019/881 introduced a mechanism for ensuring cybersecurity in accordance with the rules for preventing threats during the design of information systems rather than protecting against them and countering them. For this purpose, the European Cybersecurity Certification Framework has been created, which also applies to the means of digital transformation of justice, in particular, those created on the basis of artificial intelligence technologies. Due to the legalization of this approach to cybersecurity in the EU, the EU Regulation has created a common mechanism for the implementation of such guarantees for the protection of the rights of individuals from the risks of misuse of artificial intelligence technologies, such as accountability and controllability of algorithmic systems used in the field of justice to authorized court officials, protection of the rights of personal data subjects from disproportionate and uncontrolled use personal data by artificial intelligence, the inadmissibility of external interference in decision-making algorithms, prevention of discrimination of individuals by intelligent systems on any grounds that can identify a person, prevention of conflict and competition between artificial intelligence integrated into national judicial information and telecommunication systems in various forms, etc.

Developing the approach laid down by Regulation 2019/881 to ensuring the cybersecurity of information and telecommunications systems using artificial intelligence, on December 14, 2022, the Council of the EU approved Directive (EU) 2022/2555 on measures for a high common level of cybersecurity in the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, as well as repealing Directive (EU) 2016/1148 (NIS 2 Directive) (EU Directive 2022/2555) (hereinafter referred to as Directive 2022/2555). Directive 2022/2555 introduces measures aimed at achieving a high common level of cybersecurity in the Union to improve the internal market's functioning.

It should be noted that in accordance with Directive 2022/2555, the rule of transition from the protection of information infrastructure facilities to cyber resilience has been legalized, a separate group of provisions has been identified regarding the standardization of IT products, IT services, and processes that cover various areas of application of artificial intelligence in terms of compliance with

modern cybersecurity requirements. To achieve this goal, the European framework for certification of solutions based on artificial intelligence technologies for compliance with cybersecurity requirements has been improved. At the same time, EU Member States are obliged to further implement international ISO standards related to cybersecurity, in particular in the field of the use of artificial intelligence technologies in the administration of justice.

Thus, Directive 2022/2555 specified a number of provisions of EU Regulation 2019/881 that relate to the standardization and certification of IT solutions based on artificial intelligence technologies for cyber resilience, jurisdictional aspects of countering cyber threats, as well as requirements for guarantees of compliance with information rights in the implementation of innovative technologies.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (EU Regulation 2016/679, 2016), which provides for a broad system of guarantees of information rights of individuals related to the automated processing of their personal data, including the scope of artificial intelligence.

The guarantees of information rights in the field of artificial intelligence for the purposes of justice provided for by the General Data Protection Regulation cover the right of the personal data subject to know about the purpose, grounds, and means of personal data processing, the conditions of such processing, to consent to its implementation, or to object to such processing, except for cases when it is carried out to perform the tasks assigned to them by authorized state bodies. These guarantees also include protection against automated decision-making against the subject of personal data without informing him/her, the right to be forgotten (deletion of data about the subject of personal data from information and telecommunication systems), the right to object to profiling using artificial intelligence, in particular, in connection with the search for signs that may affect an individual when the court makes a decision taking into account the recommendations of artificial intelligence, the right to clarify data about oneself included in court case materials that can be used for processing using artificial intelligence, etc.

In accordance with the General Data Protection Regulation (EU Regulation 2016/679, 2016), these and other guarantees of the rights of personal data subjects are ensured through the mandatory implementation in the activities of personal data controllers of the rule on the need for mandatory data protection methods for the secure design of information systems and proper, secure processing of personal data.

Thus, EU law has formed a legislative mechanism for observing the information rights of individuals participating in litigation based on the design of safe, controlled, and non-discriminatory solutions based on artificial intelligence and approaches to the transparent, voluntary, informed use of such technologies in litigation, provided that human rights and freedoms are prioritized compared to the advantages of using artificial intelligence.

In the context of actualization in Ukraine, the work on the formation of the legislative framework for the development and application of artificial intelligence, the continuation of judicial and legal reform, the legislative consolidation of guarantees of observance of the information rights of individuals – participants in the judicial process in the use of artificial intelligence is an important condition for innovative transformations of national justice.

When further implementing the EU experience on these issues, it is important to cover changes in national legislation, both jurisdictional and instrumental, and ethical aspects (Zaiarnyi, p. 37, 2022).

In other words, the Verkhovna Rada of Ukraine is tasked with creating the legal basis for developing and applying artificial intelligence technologies in various spheres of public life. One of the ways to solve this problem may be the adoption of the Law of Ukraine "On the Basic Principles of the Development and Application of Artificial Intelligence Technologies". It is within the framework of this legislative act at the level of a separate article that guarantees compliance with information rights, particularly of individuals who use artificial intelligence technologies, can find their special consolidation. At the same time, it is relevant in view of the peculiarities of judicial proceedings by courts in different jurisdictions, supplementing the Law of Ukraine "On the Judiciary and the Status of Judges" with a separate article, "Application of Artificial Intelligence technologies in the activities of courts of Ukraine." The provisions of this article may cover the main directions, conditions, and principles of the use of artificial intelligence technologies by courts, guarantees of observance of the rights of participants in court proceedings when using artificial intelligence technologies, the consequences of violation of regulatory requirements for the use of this technology, etc.

In general, using artificial intelligence technologies in the justice field has more advantages than disadvantages. Potential risks can be avoided if the technology is properly enforced and ethical and legal principles are followed.

Conclusions and recommendations. The study of the peculiarities of the formation and implementation of guarantees of observance of the information rights of individuals – participants in litigation in the EU Member States gives us grounds to formulate the following conclusions and recommendations:

1. In terms of its functional potential, artificial intelligence has significant potential for optimizing court processes, including automated distribution of cases, forecasting the results of consideration, and analyzing judicial practice.

2. The benefits of using artificial intelligence primarily include speeding up procedures, reducing corruption risks, and improving access to justice.

3. EU legislation establishes an extensive system of guarantees of information rights of individuals in connection with the use of artificial intelligence, in particular, in the field of justice. These guarantees include both positive obligations of the EU Member States regarding the legislative consolidation of information rights and guarantees of their exercise by individuals in court proceedings, but also negative obligations to establish exclusive grounds for restricting these rights. By their content, these guarantees are related to the right to non-interference in private and

family life, the right to protection from automated court decision-making, the safe, voluntary, and informed use of artificial intelligence technologies to access information about the state of administration of justice, etc.

4. EU legislation is currently being developed by defining in the EU Regulation on Artificial Intelligence general guarantees of human rights in the application of artificial intelligence. At the same time, special guarantees of compliance with certain categories of information rights of individuals in connection with the use of artificial intelligence are provided at the level of acts of the European Parliament, which regulate certain types of information relations.

4. In general, the model for the implementation of guarantees of information rights in relations related to the use of artificial intelligence, enshrined in EU legislation, is based on a combination of approaches to the safe, controlled design of artificial intelligence and its responsible, ethical, transparent and voluntary application to individuals – parties to the litigation.

6. In order to improve the system of guarantees of information rights of participants in litigation when using artificial intelligence technologies, an important task is to develop the necessary legislative framework. In our opinion, it can be formed by the draft Law of Ukraine "On the Basic Principles of the Development and Application of Artificial Intelligence in Ukraine", separate additions to the Law of Ukraine "On the Judiciary and the Status of Judges", current procedural codes in terms of regulating the main directions, principles, conditions and procedures for the use of artificial intelligence in the activities of courts throughout Ukraine.

7. The State Judicial Administration of Ukraine's adoption of the procedure for using artificial intelligence technologies by courts and court apparatuses in their work is also considered justified. It is in this document that the requirements of the directions, functions, and model of artificial intelligence, which will be integrated into the Unified Judicial Information and Telecommunication System of Ukraine, the principles of its functioning, the conditions for user authorization, requirements for cybersecurity, compliance with the rights of participants in the litigation, LLP can be specified.

8. It is also important to continue activities on introducing European certification frameworks for cybersecurity components of artificial intelligence and international standards for developing and using relevant technology for justice purposes.

REFERENCES

1. AI HLEG. (2019). Ethics guidelines for a trustworthy AI. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
2. Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Retrieved from https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2020-1-of-the-committee-of-ministers-to-member-states-on-the-human-rights-impacts-of-algorithmic-systems

3. European Commission. (2018). Communication Artificial Intelligence for Europe. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>
4. European Commission. (2020). White Paper on Artificial Intelligence – A European approach to excellence and trust (COM (2020) 65 final). Retrieved from https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
5. European Commission. (2024). Declaration on European Digital Rights and Principles. Retrieved from https://commission.europa.eu/document/download/f85a4043-927f-4093-9d96-012b46631719_en
6. European Parliament. (2017). European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
7. Krot, V., & Holubovskiy, I. (2024). Shtuchnyi intelekt i sudochynstvo [Artificial intelligence and judicial process]. Yurydychna praktyka. Retrieved from <https://yur-gazeta.com/publications/practice/sudova-praktika/shtuchniy-intelekt-i-sudochinstvo.html> [in Ukrainian].
8. Reformuvannya sudovoi systemy Ukrainy: suchasni tekhnolohii ta novi pidkhody [Reforming Ukraine's judicial system: Modern technologies and new approaches]. (n.d.). Retrieved from <https://consultant.net.ua/consultant-article/7355> [in Ukrainian].
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 Artificial Intelligence Act. Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
10. Shtuchnyi intelekt u pravosuddi [Artificial intelligence in justice]. (2020). Tsentr demokratyy ta verkhovenstva prava. Kyiv. Retrieved from <https://cedem.org.ua/analytics/shtuchniy-intelekt-pravosuddia/> [in Ukrainian].
11. Verkhovna Rada Ukrainy. (2019). *Rehlament 2019/881 Yevropeiskoho Parlamientu i Rady vid 17 kvitnia 2019 roku pro Ahentstvo Yevropeiskoho Soiuzu z kiberbezpeky (ENISA) ta pro sertyfikatsiiu kiberbezpeky informatsiino-komunikatsiinykh tekhnolohii, a takozh pro skasuvannya Rehlementu (YeS) No. 526/2013 (Akty pro kiberbezpeku)* [Regulation 2019/881 of the European Parliament and of the Council on cybersecurity certification]. Retrieved from https://zakon.rada.gov.ua/laws/show/984_024-19#Text
12. Zaiarnyi, O. A. (2021). Pozasudovi formy zakhystu informatsiinykh prav pryvatnykh osib ta osnovni napriamy yikhnoi adaptatsii do standartiv Yevropeiskoho Soiuzu [Extrajudicial forms of protection of informational rights of private individuals and main directions of their adaptation to EU standards]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Yurydychni nauky*, (4)119, 32–37. Retrieved from <http://visnyk.law.knu.ua/ua/baza-nomeriv/851-pozasudovi-formy-zakhystu-informatsiinykh-prav-pryvatnykh-osib-ta-osnovni-napryamy-yikhnoyi-adaptatsiyi-do-standartiv-yevropeyskoho-soyuzu> [in Ukrainian].
13. Zaiarnyi, O. A. (2022). *Do pytannia udoskonalennia sposobiv zakhystu informatsiinykh prav fizychnykh osib u vidnosynakh, poviazanykh iz zastosuvanniam tekhnolohii shtuchnoho intelektu* [To the question of improving methods of protecting the information rights of individuals in relations associated with the use of artificial intelligence technologies]. *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Yurydychni nauky* [Bulletin of Taras Shevchenko National University of Kyiv. Legal Sciences], 1(120), 36–39. Retrieved from <http://visnyk.law.knu.ua/images/articles/7-120.pdf>
14. Zaplotynskiy, B. A. (n.d.). Elektronne sudochynstvo. Konspekt leksii [Electronic judicial process. Lecture notes]. Retrieved from <http://dspace.onua.edu.ua/bitstream/handle/11300/11107/%D0%95%D0%A1%20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf?sequence=1&isAllowed=y> [in Ukrainian].