Primljen: 28.07.2025.
Prihvaćen: 13.11.2025.
Socijalne studije / Social studies 8 (8) 2025, str. 91-113.
https://doi.org/10.58527/issn.2637-2908.8.8.91

UDK 004.8:37

Pregledni rad

ARTIFICIAL INTELLIGENCE IN EDUCATION – REVOLUTION OR RISK?

Magdalena Primorac
Undergraduate student of law, Faculty of Law, University of Mostar, Mostar, Bosnia and Herzegovina

Summary: Recent surge in the popularity of large language models has shifted discussions toward the role of artificial intelligence (AI) in the future of education. AI is transforming the learning and teaching paradigm, making it crucial to understand both the positive and negative effects of this technology on educational systems. Research on the role of AI education encompasses various topics, including analyses of AI systems applied in education, recommendations for implementing this technology into educational processes, and ethical challenges. However, significantly fewer studies address the legal aspects of AI in education. The legal dimension of AI has gained importance as more countries begin to regulate this technology. Therefore, this paper aims to analyse the current applications of AI through the General Data Protection Regulation and EU AI Act the first comprehensive regulatory framework for this technology, contributing to the understanding of legal aspects of implementing AI systems in education. This paper focuses on AI systems in education classified as unacceptable risk under the EU AI Act, such as emotion and facial recognition systems in educational contexts and high-risk systems, including automated grading, AI-driven exam monitoring, and student selection processes. Additionally, the paper explores use of AI systems not specifically designed for classroom application, potential biases of AI systems, their impact on the right to education, and challenges of personal data protection in personalized learning. Furthermore, this paper provides insights into the potential negative and risky aspects of applying AI in education. Ultimately, we highlight both, positive and negative effects of implementing AI in education and underscore the importance of legal frameworks to prevent *the misuse of this technology.*

Keywords: *AI; education; EU AI Act; GDPR; risk; bias*

E-mail: magdalena.primorac@pf.sum.ba

Thank you Note

The author would like to express her sincere gratitude to mentor dr.sc. Rialda Spahić for her help and valuable advice when writing the paper. Also, the author expresses her sincere gratitude to the Association for the Advancement of Science and Technology in Bosnia and Herzegovina for the opportunity to participate in the Student Research Project.

INTRODUCTION

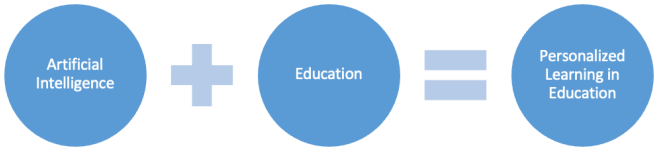
We are currently witnessing the integration of artificial intelligence (AI) into all spheres of our society, including education. The impact of this technology on the educational landscape is both revolutionary and risky. AI has presented educational systems with two key challenges:

1. Direct research efforts towards AI as an emerging technology, including necessary education to responsibly adopt and use AI.
2. Capitalisation on the potential of AI as an emerging technology and integration of AI in the education processes.

AI is showing a potential to transform the human-technology collaboration in the area of teaching and education (Kamalov, Santandreu, Gurrib, 2023). However, AI is not the only technology that has transformed education. Over the past three decades, technology has left a profound mark on education. As illustrated in Figure 1(a), the educational landscape was particularly transformed by the emergence of the Internet, making online education a new reality. Over recent years, the digital transformations in education can be categorized as the *first educational revolution*, characterized by the Internet and online learning. Integrating AI into education marks the beginning of the *second educational revolution*. AI brings numerous opportunities to the educational system, with personalized learning being the most significant. For years, knowledge has been transferred from teachers to students uniformly without substantial changes. As a result, education has remained the same for all students, regardless of their abilities and interests, with the knowledge transfer process becoming so standardized that it is nearly robotic. Through personalized learning, this technology offers the opportunity to bridge the gap between the educational system and students, bringing

knowledge closer to the individual. Figure 1(b) illustrates the assumption that AI and personalized learning will play a similar transformative role in the second educational revolution as the Internet and online learning did in the first.

(a) Online learning in education



(b) Personalized learning in education

Figure 1. *Key characteristics of the two industrial revolutions*

The integration of AI into education can be viewed through two phases. *First phase* was initiated by students through the active use of commercial AI-powered applications for performing everyday tasks, such as mathematics homework, language translation or essay writing. Characteristics of this phase are the lack of control and teachers' unawareness of the application of AI, which can potentially disrupt the learning process. First phase is also characterized by the application of AI tools that were not developed to be applied in education (for example, Google Translate, ChatGPT, and Photomath). The *second phase* of AI application involves the targeted development of technology for its use in education. This phase includes experts from various fields with a shared goal: to advance education. Its characteristics are control, awareness, and transformation of education. The second phase results in the development of various tools for implementation in education, ranging from automated grading systems to intelligent tutoring systems, with a particular emphasis on personalized learning. However, while the second phase of AI application in education brings about an educational revolution, it simultaneously carries certain risks.

This research examines the legal challenges of AI second phase of application in education. The discussion centres around the following key research questions: *How can AI potential bias affect the right to education? How can students' data be protected in digitalization and personalized learning? How risky is AI in education?* The following legal acts answer these questions: the EU AI Act which recently came into force, and the General Data Protection Regulation (hereinafter: GDPR). This paper is divided into three sections. First section analyses the EU AI Act as the first foundational legal regulation of this technology, and the application of AI in education is categorized according to the risk levels defined by the EU AI Act. The second section examines the weaknesses of AI, with a particular focus on bias and its impact on the right to education as a fundamental human right. Section three analyses the applicability of the GDPR provisions as a legal response to the application of AI in education.

Methodology

This work is based on a qualitative analysis of relevant professional and scientific literature in the field of AI and education. The methodological approach is focused on the descriptive and comparative analysis of existing research, professional articles, reports of international organizations and works that research the advantages, challenges and risks of implementing AI technologies in the educational process.

The method of content analysis was applied, which identified key concepts, patterns and thematic units related to the impact of AI on the education system, the role of teachers, personalized learning and ethical and social implications. Sources were selected according to the criteria of scientific relevance, topicality and credibility, with an emphasis on publications published in the last six years.

The goal of the methodological approach was to synthesize existing knowledge and attitudes in order to better understand the potential and risks of artificial intelligence in education, and to derive guidelines for further research and application of AI technologies in education.

EU AI Act

EU AI Act aims to establish the first comprehensive regulatory framework for AI that will extend beyond the borders of the European Union (hereinafter: EU) (Engler, 2022). Thelisson notes that similar to the GDPR, the EU AI Act will have an effect outside the EU's territory. In other words, the EU AI Act "has the potential to become the global gold standard for regulating AI" (Thelisson, 2024). The global impact of EU legal acts is known as the *Brussels Effect* stemming from the influence of the GDPR on global data protection regulations. EU AI Act forms the foundation for ensuring security and the protection of fundamental human rights in the era of AI (Almada, Petti, 2023). The EU AI Act also seeks to define the characteristics that constitute trustworthy AI. By outlining the characteristics of trustworthy AI, the aim is to highlight potential risks and identify ways to mitigate or eliminate them. In other words, trustworthy AI can be seen as a necessary condition for successfully implementing this technology. By emphasizing reliability, the EU AI Act encourages public trust in AI. It represents a strategic step toward unlocking this technology's economic and societal potential (Laux, Wachter, Mittelstadt, 2023). Table 1 shows a complex path to regulating AI as a rapidly advancing technology whose impacts were almost unexpected. In 2020, the European Council discussed AI, and a year later, in 2021, the European Commission proposed the EU AI Act, as shown in Table 1. The proposal was followed by a new step in the legal regulation of AI, with the European Council agreeing on its position on the EU AI Act in 2022. Furthermore, Table 1 shows the continuation of the discussion on AI, which resulted in an agreement between the European Council and the European Parliament. Finally, in 2024, the EU AI Act entered into force.

Table 1. *Steps in the development of the EU AI Act*

Key events in the development of the EU AI Act	Timeline
European Council discusses AI	2020
The European Commission has proposed an EU AI Act	2021
Council agrees position on EU AI Act	2022
EU Council and European Parliament reach agreement on EU AI Act	2023
Entry into force	2024

With the entry into force of the EU AI Act, Member States are required to meet certain obligations, including the establishment of bodies responsible for protecting fundamental rights and notifying the Commission and other Member States accordingly. Furthermore, starting in February 2025, bans have been applied to AI systems that pose an unacceptable risk, while the Commission is to prepare a Code of Practice by May of the same year. Provisions relating to general-purpose systems are to be enforced from August 2025, and from August 2026, the provisions for high-risk systems are to come into effect. The full application of the EU AI Act is to be achieved by August 2027. In 2029, the Commission will be able to adopt delegated acts, and by 2031, it will assess the implementation of the EU AI Act (European Parliament, 2024). Finally, it is important to note that the EU continues its efforts to regulate AI. The Vice President of the European Commission signed the Framework Convention on AI (hereinafter: the Convention), highlighting that the Convention is fully aligned with the EU AI Act. The Convention is the first legally binding international agreement on AI. It also represents global cooperation in building an approach that ensures AI systems are compatible with human rights, democracy, and the rule of law while ensuring that regulation does not hinder innovation. In the negotiations around the Convention, the EU, Council of Europe member states, Canada, the USA, Mexico, Japan, and Australia participated. The ultimate goal of the Convention is to create unified global rules and fill legal gaps that could arise due to rapid technological advancement (Vrbanus, 2024).

Risk categories according to EU AI Act

The EU AI Act represents a risk-based regulatory framework, which means that the strictness of the rules will depend on the risk that AI carries for society (Golpayegani et. al., 2023). The regulatory framework defines four risk categories: unacceptable, high, limited, and minimal risk, as shown in Illustration 2 (EU AI Act, 2024).

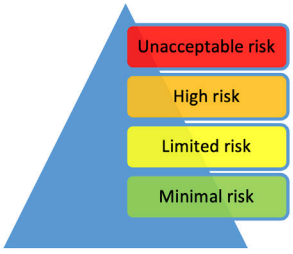


Figure 2. *Risk categories according to EU AI ACT*

Chapter II, Article 5 of the EU AI Act outlines prohibited AI systems that pose an unacceptable risk, such as biometric categorization systems, social scoring, risk assessment of an individual committing a criminal offense, emotion recognition in the workplace or educational institutions, and real-time remote biometric identification. Exceptions to this rule include the search for missing persons, kidnapping victims, or individuals who have been trafficked or sexually exploited; prevention of significant and imminent threats to life or a foreseeable terrorist attack; or identifying suspects of serious criminal offenses (EU AI Act, 2024).

The significance of these provisions for the education system is as follows: the ban on AI systems that pose an unacceptable risk excludes the possibility of facial and emotion recognition systems being implemented in educational institutions.

Furthermore, Chapter III of the EU AI Act addresses high-risk systems, such as those used for individual assessments, decision-making, or automated data processing to evaluate a person (EU AI Act, 2024). In education, AI systems designed to determine access to or admission into educational institutions could pose a high risk, primarily due to improper design and usage. Lawmakers have acknowledged this risk, considering it necessary to categorize such systems as high-risk because they "*can determine an individual's educational and professional course of life, thereby impacting their ability to secure a livelihood*."

As previously noted, improper design and application could lead to violations of fundamental human rights, such as the right to education and training and the right to be free from discrimination (Kempf, Rauer, 2024)

Limited risk under the EU AI Act applies, for example, to chatbots. It is necessary to comply with the Copyright Directive for their development. Individuals must be informed that they are interacting with a non-human system when used (EU AI Act). Minimal risk under the EU AI Act includes using popular AI tools like ChatGPT. The implementation and development of chatbots for educational purposes do not pose significant risks; therefore, they can be used in educational institutions. Once again, with the EU AI Act, the EU has played a key role in adapting legal frameworks to the digital age and protecting human rights amidst the rapid development of new technologies.

Application of AI in education through risk categories according to EU AI Act

With the continuous influx of new technologies that can be used in education, it is crucial to assess which technologies can improve education and where it is necessary to draw the boundaries of applying specific technologies (Lai, Bower, 2019). An example of a technology used in education that raises the question, "Does it have a place in the classroom?" is facial and emotion recognition technology. China is an example of a country that uses the Class Care System, which classifies each student's behaviour based on facial expressions. Advocates of using this technology in education state that the advantage is that it allows teachers to recognize when a student needs help. Namely, this system classifies a student into a specific category based on facial expressions (for example, interaction with another student). Each student receives a weekly score that can be accessed via a mobile application. Also, in addition to the students, teachers, parents, and school management have access to the weekly scores and can thus find out how much time the students spend in each category (Yujie, 2019).

However, applying facial and emotion recognition technology may create a sense of pressure for students to behave in a certain way, potentially leading to inaccurate results. The mere presence of a camera in the classroom can result in unnatural behaviour from students and teachers. According to the EU AI Act, using AI systems to detect individuals' emotional states in the workplace and educational settings is prohibited. In this case, such AI systems cannot be used in educational institutions primarily because they are designed for student education but also constitute the workplace for teachers. Accordingly, facial and emotion recognition technologies cannot be used in educational institutions within EU member states. Systems like the Class Care System cannot be found in EU classrooms as they are prohibited and categorized as unacceptable risks under the EU AI Act.

Furthermore, AI systems applied in education often fall into the high-risk category. For instance, automated grading is considered a high-risk system. AI transforms traditional grading in two ways:

1. Grading can be automated through the application of AI, which contributes to the implementation of adaptive teaching strategies. It is also assumed

that using automated grading with feedback could allow for identifying gaps in conceptual development among a larger number of students within a shorter time frame than previously possible. Schools in France have already begun implementing automated grading. It is particularly used for essay assessments to accelerate grading and reduce subjectivity (De Gree, 2025).

2. Students using AI systems to complete tasks, such as writing essays, create "detectors" of such content. In practice, it is difficult to discern when a text is AI-generated and when it results from human intellectual effort. Therefore, "detectors" facilitate the recognition of generated content. The use of AI in detecting "artificial" content will impact a student's grade due to their use of technology, thereby changing the grading process.

Along with automated grading, AI systems used for monitoring students during tests, making decisions about student admissions, and determining whether students meet entry requirements also fall into the high-risk category under the EU AI Act. High-risk AI systems are not prohibited, as is the case with unacceptable risks. However, high-risk systems are subject to stricter conditions and obligations.

AI systems categorized as limited risk under the EU AI Act include chatbots and intelligent tutoring systems, with a requirement for transparency, meaning that individuals must be informed of their interaction with AI (unless it is self-evident). For example, Jill Watson is an "artificial" assistant capable of answering student questions and freeing professors from routine tasks. However, the integration of this system into the educational process went unnoticed, as students did not suspect that they were interacting with AI (Taneja, 2024). With the further advancement of AI, it will become increasingly difficult to distinguish the "artificial" from the real, making it crucial to inform individuals when interacting with AI. Finally, using "commercial applications" powered by AI in education would fall under the minimal risk category. "Commercial applications" refer to AI-assisted tools that students carry in their pockets. These include popular apps such as Photomath, ChatGPT, and similar tools that students use to facilitate task completion. Such apps are not necessarily designed for students and education, but they find their way into the classroom. AI-assisted apps are most commonly used secretly by students to speed up or ease task completion, tests, and essay writing. We could say that students independently integrate such tools into their

educational process, which could significantly influence the future of learning. When solving a math problem at their desk, students might use a calculator and, under the desk, Photomath. Such tools create a false impression that the student has mastered the material, as teachers remain unaware of the use of AI tools.

Therefore, teachers must allow AI tools to be present on desks, which would help them remain aware that the student needs assistance, even if the correct result appears on paper. Additionally, teachers can show students that technology is imperfect and has flaws, thereby eliminating the perception that technology is superior to human knowledge. Otherwise, we may find ourselves in a situation where AI will not necessarily become smarter over time, but we will become more dependent. When we encounter generations whose success in solving problem tasks depends on technology, the "blame" will not lie with AI but with us. However, will we be aware of our responsibility in their development?

The application of AI in education has both positive and negative effects on the educational system. The positive effects of this technology include time savings for teachers through automated grading and student selection, bringing knowledge closer to the student through personalized learning, emotion recognition technology allowing teachers to notice when students need help, and time-saving for students using AI to complete tasks. However, these applications also have negative effects: in personalized learning, the challenge of protecting personal data, the potential for AI to influence students' future through automated grading and selection, the possibility that emotion recognition technology could cause discomfort for students, and excessive reliance on AI assistance may make students' success dependent on technology.

Finally, teachers need to be made aware that they and their educational institutions will be responsible for the adequate and correct use of AI tools in their work. First, they should be aware of which types of use are permitted and prohibited and that they require additional assessment steps. Educational institutions should also educate students about the risks that the technology poses.

The EU AI Act is only the initial phase of regulating AI. The next phase involves the challenging process of implementing the EU AI Act into the national legislation of the Member States.

"The Achilles' heel" of AI

The capabilities of AI simultaneously fascinate, evoke fear, and create enormous expectations. However, despite its numerous advantages, this technology has limitations and faces several weaknesses:

1. *Dependence on data*: AI heavily relies on vast amounts of data. While humans can learn from a single example (one-shot learning), AI typically requires large datasets with labelled examples for effective generalization. If AI systems are trained on copyright-protected content, legal rights issues may arise even before implementation. Ongoing court cases regarding copyright infringement during AI training are likely to impact the development of this technology. Should courts determine that AI training constitutes copyright infringement, the technology may lose access to essential "learning material." Conversely, if no infringement is found, the internet may become a "safe zone" for data collection through practices like data mining (Teng, 2019).

2. *Adaptation to New Situations and Complex Training*: Flexibility and adaptability represent another critical weakness of AI systems. Human intelligence excels in adapting to new situations and environments, leveraging complex reasoning and intuition. In contrast, AI, especially traditional machine learning models, tends to be narrowly specialized and struggles with tasks outside its training domain. Additionally, the process of training AI is inherently complex. The core of AI learning lies in model training, where selected algorithms are "fed" with curated datasets to identify patterns, correlations, and dependencies within the data. During training, the algorithm iteratively adjusts its internal parameters to refine its ability to predict or classify based on observed patterns. This process involves comparing the model's predictions with known outcomes in the training data and adjusting parameters to minimize errors or improve accuracy. Once trained, the model undergoes evaluation to assess its performance and generalization capabilities. Evaluation includes testing the model on a separate dataset (known as the validation or test set) that is not used during training. This step helps determine how well the model performs on unseen data, offering insights into its robustness and reliability in real-world applications. Iterative refinement may occur based on evaluation results, with algorithm adjustments or preprocessing techniques to enhance performance further (Flasiński, 2016).

3. *The Black Box Problem:* The lack of transparency in AI systems complicates their integration into sensitive domains such as data processing or education. While deep learning and neural networks have revolutionized AI capabilities, understanding how these models make decisions remains elusive. This "black box" problem undermines transparency and interpretability. In science, computing, and engineering, a black box refers to a system that can be observed in terms of its inputs and outputs (or transfer characteristics) without any knowledge of its internal workings. The opacity of these algorithms hinders the establishment of trust in AI systems. Trust in AI systems is further compromised by their inability to explain their reasoning or justify outcomes beyond statistical correlations (Teng, 2019).

4. *Hallucinations*: AI's notable weakness is hallucinations and potential biases. For instance, popular models such as ChatGPT, when lacking knowledge on a particular topic, may generate fabricated and absurd responses that appear accurate to the user. Such instances exemplify hallucinations, highlighting the inherent limitations of AI's reliability. On the other hand, potential biases in AI systems represent a significant drawback that demands careful attention. If unaddressed, these biases can undermine the credibility and fairness of AI applications, emphasizing the need for rigorous oversight and mitigation strategies.

Bias in AI and right to education

The vast amounts of data processed and learned from by AI are essential for the efficiency and advancement of this technology. The effectiveness of AI systems fundamentally depends on the availability, quality, and diversity of data. Data is the "fuel" driving AI algorithms, enabling them to learn, adapt, and perform tasks across various domains. The quality of this data, i.e., its cleanliness, accuracy, and representativeness, determines the reliability of AI systems. Despite its transformative potential, AI's reliance on data introduces several challenges, including bias. The bias inherent in training data can result in discriminatory outcomes, perpetuating social inequalities if not appropriately addressed. Ensuring data diversity helps mitigate these biases and promotes fairness in AI systems (Nivedhaa, 2024). AI bias can undermine fundamental human

rights, including the right to education. The right to education is enshrined in international human rights instruments, such as the Universal Declaration of Human Rights, the European Convention on Human Rights, and the Convention on the Rights of the Child. This right encompasses access to quality education without discrimination. Algorithmic bias jeopardizes this right by creating unequal educational opportunities and outcomes. Biased models can lead to disproportionate interventions for particular groups (e.g., minorities and women), resulting in stigmatization and reduced educational attainment (Baker & Hawn, 2021). Furthermore, while AI has the potential to transform education by providing personalized learning experiences, automating administrative tasks, and facilitating access to educational resources, AI bias can have significant negative implications for education. For instance, AI-driven educational tools and platforms may not be equally accessible to all students. Students from low-income families or remote areas may lack the necessary technology or internet access to benefit from AI-based education (Shah, 2023). Additionally, AI systems that perpetuate societal biases can reinforce harmful stereotypes. For example, an "artificial" instructor providing different types of feedback to students based on their gender or ethnicity could strengthen existing stereotypes and hinder the educational progress of affected students. Similarly, AI systems that predict student success based on biased historical data may unfairly disadvantage students due to their background (Shah, 2023).

To safeguard the right to education, addressing the root causes of algorithmic bias is essential. According to Baker and Hawn (2021), the solutions include:

1. *Improving the quality and diversity of data:* It is crucial to ensure that training data for AI systems is diverse and representative of all student groups. It can help mitigate biases arising from unrepresentative or distorted datasets.
2. *Algorithmic transparency and accountability:* Implementing transparent algorithms and creating decision-making processes in AI systems that are understandable to stakeholders can help identify and correct biases. Additionally, establishing accountability mechanisms can ensure that biases are promptly detected and addressed.
3. *Incorporating ethical considerations:* Developing ethical guidelines for using AI in education can help align AI applications with principles of fairness and

equity. It includes considering the potential impacts of AI systems on different student groups and taking steps to minimize harm.

4. *Continuous monitoring and evaluation:* Regular monitoring and evaluation of AI systems in education can help detect biases early and ensure the implementation of corrective actions. This ongoing process can contribute to maintaining the fairness and effectiveness of AI applications.

The bias of AI has shown itself in practice. Namely, the AI systems used in the United States have shown a bias towards black and Latin American students. When assessing success, the algorithms incorrectly predicted failure for these students. Model bias can deny admission to students based on race if such models are left to make college admissions decisions. Also, the models are used to advise students when choosing a future college. biased models may advise black and Hispanic students to choose easier majors or courses (Gándara et. al., 2024). In the United Kingdom, the application of artificial intelligence in education led to a debacle and confirmed the bias of this technology. The model favored students from private schools and affluent areas while leaving high-achieving students from free, state schools disproportionately affected. many students were denied university places because of wrong exam results (Shead, 2020).

General Data Protection Regulation in era of digitalization and personalized learning in education

The emergence of information and communication technologies has revolutionized various sectors, including education. Personalization and digitalization in education have enabled tailored learning experiences, improved accessibility, and streamlined administrative processes. However, these advancements have also brought significant challenges, particularly regarding protecting personal data. Data protection mechanisms have evolved significantly over time. At the European level, personal data protection was comprehensively regulated for the last time in 1995. Since then, information and communication technologies have drastically changed everyday activities and the handling of personal data. Data centralization and online accessibility have become commonplace, affecting various sectors, including education. This transformation means that personal

data about individuals is now primarily stored digitally and can be accessed remotely. The General Data Protection Regulation (GDPR), introduced in 2016 and enforced in 2018, marked a significant step forward in personal data protection. The goal of the GDPR is to standardize data privacy laws across the EU, empower EU citizens regarding their data privacy, and reshape organizational practices related to data access (Olimid, Olimid, 2021:18).

The GDPR establishes a harmonized legal framework across all EU member states, focusing on protecting fundamental human rights and processing personal data. Educational institutions, including higher education institutions and state schools, operate under the GDPR as public authorities or non-public entities subject to specific local controls. This classification impacts how they manage and process personal data. The GDPR imposes stringent standards for protecting data subjects and mandates specific roles, such as data protection officers, who oversee compliance. The primary challenge lies in balancing the collection and use of data for educational purposes while ensuring robust protection of individual privacy rights. Educational institutions collect two primary types of personal data (ibid.:20).

1. Common personal data: This includes names, addresses, email addresses, student and staff identification data, academic records, and financial information.
2. Special categories of personal data: This includes more sensitive data such as biometric, genetic, and health-related information.

The GDPR sets strict regulations for processing these types of data, focusing on lawful processing, consent, and data minimization. For example, Article 9 of the GDPR regulates the processing of special categories of personal data, requiring explicit consent or specific conditions under which such data can be processed. Furthermore, the GDPR establishes several rights for data subjects that educational institutions must comply with, including (ibid.:16):

1. *Right to information:* Data subjects must be informed about how their data is processed.
2. *Right of access:* Data subjects can request access to their data
3. *Right to correction and deletion:* Under certain conditions, data subjects can

request corrections of inaccurate data and deletion of their data.

4. *Right to object:* Data subjects can object to processing their data in certain scenarios.
5. *Right to data portability:* Data subjects can transfer their data between data controllers.

Furthermore, Article 9 of the GDPR served as a response to the application of facial recognition technology in education, confirming the applicability of the GDPR to AI. Technology development has enabled the "migration" of education into the virtual space, with online education becoming a new reality. Online education brings challenges, particularly in the context of cheating during exams. In order to prevent identity fraud during exam access, higher education institutions in Spain began applying facial recognition technology. However, this practice was unsuccessful, and the data protection authority determined a violation of Article 9 of the GDPR, as students had no choice or consent to be exposed to facial recognition technology (Catalan DPA, 2022).

In the digital age, educational institutions collect vast amounts of personal data, including names, contact details, academic records, and behavioral data, through learning management systems, making personal data one of the most valuable resources. The GDPR mandates that institutions obtain explicit consent from individuals before processing their data. This requirement challenges ensuring informed and voluntary consent, especially in environments where students or parents may feel compelled to consent to data collection. Ensuring the security and proper storage of personal data is another significant challenge. Educational institutions must implement robust security measures to protect data from unauthorized access, breaches, and cyberattacks. The GDPR requires institutions to demonstrate transparency in their data processing practices, including collecting, storing, and deleting data, which involves developing comprehensive internal frameworks and control mechanisms. Educational institutions often collaborate internationally, leading to cross-border data transfers. The GDPR stipulates that personal data can only be transferred to countries with adequate legal safeguards. This provision complicates data sharing with countries that do not meet the GDPR standards, such as the United States unless specific agreements like the EU-US Privacy Shield are in place (Spalević, Vićentijević,

2022). The application of AI in education often involves collecting and analysing large amounts of personal data. If not handled properly, this can lead to privacy violations and the misuse of sensitive data (Baker, Hawn, 2021). The GDPR can be seen as a complement to the EU AI Act in the context of personal data protection. The provisions of the GDPR can be applied to AI systems used in education. Through the GDPR provisions, educational institutions must ensure that their AI-driven systems include human oversight, providing mechanisms for students to challenge and seek human intervention in automated decisions. It helps mitigate the risks associated with high-risk technologies outlined in the EU AI Act. Moreover, human oversight ensures the deletion of personal data upon the request of students or parents, thereby fulfilling the right to be forgotten guaranteed by Article 17 of the GDPR. This balance between automation and human oversight is crucial for maintaining trust and ensuring compliance with the GDPR. The ethical implications in education extend beyond privacy concerns. As technology matures, it is essential to develop comprehensive data governance frameworks that address data ownership, transparency, and accountability questions. Educators and policymakers must establish clear guidelines regarding who owns the data and how it can be used. Effective data management requires a strategic approach that includes stakeholder engagement, clear communication of data practices, and continuous data usage monitoring and evaluation. It ensures the ethical and responsible use of data, reducing the risk of bias, discrimination, and inequality in educational outcomes (Arante, 2024:525).

CONCLUSION

The emergence of the Internet has transformed the educational landscape, and the development and application of AI in education represents a new phase in the educational revolution. Every transformation brings opportunities and challenges, as does the AI-driven transformation we currently witness. Although we may seem surrounded by new and unfamiliar technologies that we still need to integrate into education, the reality is somewhat different. Students have already begun applying AI in education, and the technology has been changing the learning and teaching paradigm for years. AI in education is not something that is about to happen; it has already left its mark on education. Through the analysis of AI applications so far, this paper shows that not all technologies used in education are high-risk. Technology in education is considered high-risk when it makes decisions that can impact students' future, such as automated grading, selection in entrance exams, or monitoring during tests. This paper also demonstrates that, in addition to high-risk systems, there are AI systems in education that fall under unauthorized risk and those that fall into limited or minimal risk categories. Systematizing AI systems in education into risk categories contributes to understanding the challenges of AI's application in education. Additionally, this paper shows that legal acts like the GDPR, although not specifically designed to regulate AI, can serve as a legal response to the application of this technology in education.

Furthermore, technology has its financial side, meaning that AI-driven educational tools and platforms will not be equally accessible to all students. Students with low incomes lack the resources to acquire the necessary technology. Therefore, it is crucial to consider the financial situation of the students attending educational institutions when applying for AI. Also, bias resulting from training AI systems on poor-quality data can lead to discrimination against certain groups of students, thus undermining their right to education.

Legal regulation can successfully mitigate most of the challenges and risks AI poses. Setting standards that AI must meet before being applied in education can prevent problems related to inadequate design. Establishing limits for applying this technology prevents violations of fundamental human rights. Additionally, adapting educational curricula ensures that all students have access to knowledge

about AI. Regardless of their field of study, students must not be discriminated against for knowledge of this technology. Without knowledge of digital rights, students and educators cannot identify violations of those rights. Therefore, it is essential to raise awareness that digital rights are inseparable from human rights in the era of new technologies. Legal regulation significantly influences the development and application of AI, and it is crucial to consider these impacts and ensure that legal regulation does not hinder innovation. Implementing AI in education ushers the educational system into another risky revolution. The moment AI enters educational institutions marks the beginning of a revolution and a risk.

In order to avoid the negative effects of the application of artificial intelligence, the key recommendations are: it is necessary to carry out training on the responsible use of AI in education, the establishment of mechanisms for monitoring the application of AI in education, human supervision on AI, continuous professional development of teachers on the application of these technologies in the educational process and higher education institutions should develop their own policies and strategies on the responsible use of AI.

REFERENCES

- Almada, Marco and Nicolas Peti. 2023. „The EU AI Act: a medley of product safety and fundamental rights?“ *Robert Schuman Centre for Advanced Studies Research Paper* 23 (59): 7-27.
- Arantes, Janine. 2024. „Digital twins and the terminology of personalization or personalized learning in educational policy: A discussion paper“ *Policy Futures in Education Policy* 22 (4): 524-543.
- Baker, Ryan and Aron Hawn. 2021. „Algorithmic Bias in Education“ *International Journal of Artificial Intelligence in Education* 32 (4): 1052–1092.
- Catalonia, APDCAT. 2024. *PS41/2022* Accessed 22, August 2025 (https://gdprhub.eu/index.php?title=APDCAT_(Catalonia)_-_PS_41/2022&mtc=today)
- De Gree, Adam. 2025. Automated Grading for Subjective Assessments: Challenges and Solutions. *Assessment Technology Blog*, Accessed July, 27, 2025 (https://www.taotesting.com/blog/automated-grading-for-subjective-assessments-challenges-and-solutions/)
- Flasiński, Mariusz. 2016. Introduction to Artificial Intelligence. Springer, International Publishing: Cham
- Gándara, Denis, Hadis Anahideh, Matthew Ison and Lorenzo Picchiarini. 2024. „Inside the Black Box: Detecting and Mitigating Algorithmic Bias Across Racialized Groups in College Student-Success Prediction” *AREA Open* 10 (1): 1–15.
- Golpayegani, Delaram, Harshvardhan Pandit, and David Lewis. 2023. “To Be High-Risk, or Not To Be—Semantic Specifications and Implications of the AI Act’s High-Risk AI Applications and Harmonised Standards” *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* Accessed July 20, 2025 (https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594050)
- Jennifer Lai and Matt Bower. 2019. „How is the use of technology in education evaluated? A systematic review“ *Computers & Education* 133 (19): 27-42.
- Johan Laux, Sandra Wachter and Brent Mittelstadt. 2024. „Three pathways for standardisation and ethical disclosure by default under the European Union Artificial intelligence Act“ *Computer Law and Security Review* 53 (24): 3-33.

- Kamalov, Firuz, David Santandreu Calonge and Ikhlaas Gurrib. 2023. „New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution“ *Computer Science: Computers and Society* 15 (16): 2-36.
- Nils Rauer and Anna-Lena Kempf. 2024. „A guide to high-risk AI systems under the EU AI Act“ Accessed July 24, 2025 (https://www.pinsentmasons.com/out-law/guides/guide-to-high-risk-ai-systems-under-the-eu-ai-act)
- Nivedhaa, N. 2024. „A comprehensive review of ai's dependence on dana“ International Journal of Artificial Intelligence and Data Science 1 (1): 1-11.
- Olimid, Anca and Daniel Olimid. 2021. „Subjects' rights and data privacy: GDPR's impact on educational institutions“ *Journal of Contemporary Education Theory and Research*, 5 (2): 15-20.
- 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. Accessed June 24, 2024 (https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng)
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised 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), *Official Journal L 2024/1689*. Accesed July 24, 2025 (https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng)
- Shah, Pirten. 2023. AI and the Future of Education: Teaching in the Age of Artificial Intelligence. Jossey-Bass: Hoboken.
- Shead, Sam. 2020. "How a computer algorithm caused a grading crisis in British schools" Accessed August 5, 2024 (https://www.cnbc.com/2020/08/21/computer-algorithm-caused-a-grading-crisis-in-british-schools.html)
- Spalević, Žaklina and Kosana Vićentijević. 2022. „GDPR and challenges of personal data protection“ *The European Journal of Applied Economics* 19 (1): 55-65.

- Taneja, Karan, Pratyusha Maiti, Sandeep Kakar, Pranava Guruprasad, Sanjeev Rao and Ashok Goel. 2024. „Jill watson: A virtual teaching assistant powered by chatgpt“ *Computer Science, Artificial Intelligence* 17 (24): 324-337.
- Thelisson, Eva and Himanshu Verma. (2024). Conformity assessment under the EU AI Act general approach. *AI and Ethics* 4: 113.-121.
- Vrbanus, Sandro. 2024. „Potpisana međunarodna Okvirna konvencija o umjetnoj inteligenciji“ Accessed August 26, 2024 (https://www.bug.hr/propisi/potpisana-medjunarodna-okvirna-konvencija-o-umjetnoj-inteligenciji-43322)
- Xaiofei Teng. 2019. „Discussion About Artificial Intelligence’s Advantages and Disadvantages Compete with Natural Intelligence“ *Journal of Physics Conference Series* 1187 (3): 2-7.
- Yujie, Xue. 2019. “Camera Above the Classroom“ Accessed July 28, 2024 (https://www.sixthtone.com/news/1003759)

UMJETNA INTELIGENCIJA U OBRAZOVANJU – REVOLUCIJA ILI RIZIK?

Sažetak: Nedavna eksplozija popularnosti velikih jezičnih modela usmjerila je rasprave o ulozi umjetne inteligencije u budućnosti obrazovanja. Umjetna inteligencija mijenja paradigmu učenja i poučavanja zato je ključno razumjeti pozitivne i negativne učinke ove tehnologije za obrazovni sustav. Istraživanja o ulozi umjetne inteligencije u obrazovanju obuhvaćaju širok spektar tema, od analize sustava umjetne inteligencije koji se primjenjuju u obrazovanju, preko preporuka za implementaciju ove tehnologije u obrazovni proces, do etičkih izazova. Međutim, znatno manje istraživanja obuhvaća pravnu stranu primjene umjetne inteligencije u obrazovanju. Pravna strana umjetne inteligencije postaje značajnija otkako sve više država započinje s pravnom regulacijom ove tehnologije. Stoga ovaj rad ima za cilj analizirati dosadašnju primjenu umjetne inteligencije kroz Opću uredbu o zaštiti osobnih podataka i Akt o umjetnoj inteligenciji kao prvi sveobuhvatni regulator ove tehnologije kako bi se pridonijelo razumijevanju pravne strane implementacije sustava umjetne inteligencije u obrazovanje. Rad se usredotočuje na primjenu sustava umjetne inteligencije u obrazovanju koja spada u neprihvatljiv rizik prema Aktu o umjetnoj inteligenciji kao što su sustavi za prepoznavanje emocija i lica u obrazovanju te visokorizične sustave kao što su automatsko ocjenjivanje, nadziranje učenika tijekom ispita putem sustava umjetne inteligencije, selekciju učenika sustavima umjetne inteligencije. Također, kroz rad se otvara tema primjene sustava umjetne inteligencije koji nisu ciljano razvijeni da se pronađu u učionici, potencijalne pristranosti sustava umjetne inteligencije i njena utjecaja na pravo na obrazovanje te izazove zaštite osobnih podataka kroz personalizaciju obrazovanja. To omogućuje izvještavanje o mogućim negativnim i rizičnim aspektima primjene umjetne inteligencije u obrazovanju. U konačnici, rad ističe pozitivne i negativne učinke implementacije umjetne inteligencije u obrazovanje i ističe važnost zakonskih okvira koji će spriječiti zloupotrebe ove tehnologije.

Ključne riječi: *umjetna inteligencija, obrazovanje, Akt o umjetnoj inteligenciji, Opća uredba o zaštiti osobnih podataka, rizik, pristranost*