FDB | FACULTY OF DIPLOMACY AND SECURITY

INTERNATIONAL SCIENTIFIC CONFERENCE

BINS 2025
SECURITY CHALLENGES OF THE NEW WORLD

Co-funded by the European Union

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICES

CONFERENCE PROCEEDINGS

BELGRADE, MAY 8 - 9, 2025

INTERNATIONAL SCIENTIFIC CONFERENCE
BINS 2025

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICE

FACULTY OF DIPLOMACY AND SECURITY
BELGRADE, 2025.

INTERNATIONAL SCIENTIFIC CONFERENCE - BINS 2025

CONFERENCE PROOCEEDINGS

TRANSDISCIPLINARITY OF SECURITY STUDIES AND PRACTICE

Publisher:
FACULTY OF DIPLOMACY AND SECURITY
Milorada Ekmečića 2, Belgrade
www.fdb.edu.rs

For publisher:
Prof. Dr. Radojica Lazić

Editor:
Prof. Dr. Milica Bošković

Technical editor:
Branko Velov, MA

Cover:
Prof. Dr. Aleksandra Arvanitidis

Proofreading:
Mina Suknović, MA

Translation:
Doc. Dr. Katarina Šmakić

E-edition:
Faculty of Diplomacy and Security, Belgrade

Circulation:
100 copies

ISBN-978-86-87545-51-9

Belgrade, 2025.

Mina Zirojević[1]
Darko M. Marković[2]

DARK NET, SOCIAL MEDIA AND EXTREMISM

Abstract

The recent IS attack in Jakarta highlights the increasing use of the dark web to conceal and protect terrorist communications. Radicalization via Internet networks, the spread of false and half-truths, and the recruitment of new members into terrorist organizations via the Internet have long been well documented. In June 2015, Beatrice Burton wrote about IS's superior messaging and engagement capabilities, which should direct us to achieve at least equal effectiveness in countering such activities. There is ample evidence that one of the reasons for the lack of success in the fight against radical extremism is the overanalysis of narratives. Responses to these direct narratives are often too academic and research-oriented, failing to reach the target groups. Most extremist movements convey a relatively simple message – one that is easy to understand and easy to accept. An effective counter-narrative should consist exclusively of photos, videos and 140 characters. No more, no less. In this paper, we answer the question of what an effective response should entail and what the success of its implementation depends on, despite potential challenges and obstacles.

Keywords*: Terrorism, Dark Web, Media, Narrative.*

INTRODUCTION

The digital world has changed the way we live, connect and interact. While once the fight against extremism meant following physical clues – meetings in secret rooms or letters passed through intermediaries – today the fight has moved to the invisible paths of the Dark Net and noisy social media platforms. It didn't take long for extremists to realize the power of these tools: from encrypted messages to viral videos recruiting young people from their bedrooms. Although it might seem at first glance, this is not just a technological change, but a new kind of struggle for simple messages to attract people's attention and loyalty. On the other hand, security forces and institutions often flounder, stuck in complex analyzes and responses that do not reach those for whom they are intended. This disparity between extremist skill and institutional inertia raises the question: how to restore balance in this struggle?

1 Institute of Comparative Law, Belgrade, Serbia, mina.zirojevic@gmail.com

2 Faculty of Law for Commerce and Judiciary in Novi Sad, University of Business Academy in Novi Sad, Serbia, darko.bg.ns@gmail.com

The aim of this research is to show why conventional responses to extremism fail and to offer a practical solution – a counter-narrative that can compete with extremist messages on their turf. It is not enough to understand how the Dark Net and social media work as weapons in the hands of terrorists; it is necessary to discover what we can do to surpass them. The paper starts from the assumption that the strength of extremists lies in the simplicity and emotions with which they win over the audience, while the official answers lose their impact due to excessive complexity and lack of human touch. The idea is not to create another complex plan that will end up in a drawer, but to offer something that can be implemented immediately - messages that fit into 140 characters, accompanied by images and videos that speak the language of communities. Therefore, the goal of this work is to show how powerful the understanding of people and their needs is as an approach in the effort to stop extremism.

The methodological process that led to these conclusions relies on a combination of analysis of existing examples and practical thinking about what works in the real world. First, it studied how extremists use the Dark Net and social media, looking at specific cases such as the Jakarta attack or Facebook recruitment. It then discusses why current responses – from academic studies to institutional campaigns – are not delivering, focusing on their weaknesses such as over-theorizing and neglecting the local context. Through this analysis, recurring patterns have been observed: extremists win because they are fast and close to the people, while institutions fall behind because they are slow and distant. Based on this, a counter-narrative built on simplicity and emotion is proposed and tested through examples of messages and visuals that could work. The work does not rely on complex statistics or models, but on the logic of everyday life – what would make someone choose a community instead of hatred that provides them with a sense of belonging, authenticity and an opportunity to express themselves through some activity. Finally, it discusses how this approach could be implemented and what obstacles stand in the way, giving a practical view of how to move from idea to action.

This paper is not just another theoretical discussion – it is a call to return the fight against extremism to where it is really fought: in the digital space where messages are born and spread. While extremists use the web as a megaphone for their ideas, we must learn to use it as a bridge to the public. If we can understand what drives them and give them something better to believe in, we can turn the tide of this fight. Everything starts with a simple step - speaking in a language that is heard and understood.

DARK NET AND SOCIAL MEDIA AS TOOLS OF EXTREMISM

Connectivity and the wider digital realm play a central role in shaping modern society. During the 21st century, the digitalization process brought, initially, many good

things, such as the expansion of economic opportunities and the exchange of cultural goods, the connection of different cultures, and improved access to information and services for individuals around the world who would otherwise lack such opportunities. According to the International Telecommunication Union (ITU), in 2023, 67 percent of the world's population – or 5.4 billion people – had access to cyberspace (International Telecommunication Union [ITU], 2023). Today, that number is much higher. With the growth of the number of participants online, there is more and more misuse of it, so now all the criminal activities that we have in real life, we have online in an even worse form. This development has allowed extremists to use the Dark Net and social media as key tools for coordination, propaganda and radicalization (Weimann, 2016).

Increased concern about illegal activity on the dark web has been fueled by the emergence of a wider "criminal underworld" – online communities to coordinate illegal activity. The inclusion of the dark web is natural for this underground, as is its expansion into the wider ecosystem of the Internet, including increasingly encrypted communication platforms. The terms Deep Web, Deep Net, Invisible Net or Dark Web refer to the content of the deep part of the Internet that is not indexed by standard search engines. The deepest layers of the deep web, known as the dark web, contain content that is deliberately hidden, including illegal and anti-social information, such as terrorist communications (Chen et al., 2008). For example, Al Qaeda used encrypted messages left in the "drafts" folders of webmail services to avoid intelligence surveillance, while "Silk Road" coordinated illegal activities, earning over $1.2 billion in bitcoins before the arrest of founder Ross Ulbricht in 2013 (Zirojević Fatić, 2011).

Some phenomena are known or more advanced in the cyber world, for example the phenomenon known as "crime-as-a-service" - a business model in which criminals offer products or services to potential customers in exchange for a non-monetary fee. This model, also called "cyber-crime-as-a-service", allows individuals with varying degrees of technical expertise to engage in the criminal world alone or within a group structured as legitimate companies that employ teams of programmers, engineers and technical support representatives. Although this model is widespread in cybercrime, extremists adapt it for coordination and financing, facilitating cooperation among terrorists around the world and expanding the geographic scope of their activities (Zirojević Fatić, 2011).

The recent IS attack in Jakarta, Indonesia, shows the increasing use of the darknet to conceal and protect terrorist communications (Weimann, 2016). IS used encrypted platforms to plan and spread propaganda, while social media served to recruit and amplify messages. According to the "theater of terror" theory, such attacks are carefully designed to attract global attention, using simple, dramatic narratives (Jenkins, 1975, as cited in Zirojević Fatić, 2011). Hezbollah, for example, uses websites to publish "martyr" statistics and psychological pressure on Israelis, while Hamas recruits through Facebook and uses Google Earth to plan attacks, as seen in Mumbai in 2008 (Zirojevic Fatić, 2011).

If we go back to the beginnings of the Internet, we will see that its use was reduced to sending false truths and half-truths, as well as mutual communications between members of terrorist organizations. Of course, it is also related to the level of technological development and the possibility of content creation. Later, especially during the corona virus pandemic, the need to recruit new members through the network developed (Wimmer, 2016). However, the development of technology brought competent institutions to the door of criminals, and they fled to the edges of the Internet, that is, to the part that we colloquially call the "dark network" or darknet. Today, on the dark side of the Internet world, radicalization via the Internet, sending false and half-truths, recruiting new members of terrorist organizations, hiding and collecting money via the Internet, which has long been well documented (Weimann, 2016). Research confirms the rise of these activities on the Dark Web (Chen et al., 2008).

Security forces are still struggling to adequately respond to this threat. The main reason for the lack of success in the fight against radical extremism is the excessive analysis of the narrative, that is, the complexity of the answers. Terrorists spread propaganda and attract new supporters with simple language, facts and images, and the responses to this simple narrative are generally overly scientific, investigative and do not reach the target groups (Berton, 2015, as cited in Weimann, 2016). Most extremist movements carry a relatively simple message – a message that is easy to understand and adopt. An effective counternarrative should consist of only photos, videos and no more than 140 characters, opposing extremist propaganda on the same ground (Malik, 2018).

PROBLEMS WITH CONVENTIONAL RESPONSES TO EXTREMISM

The Internet, like an ocean that encompasses the surface, deep and dark webs (Chen et al., 2008), poses complex challenges for the fight against extremism. While terrorist groups like IS skillfully use the Dark Net and social media to spread their messages (Weimann, 2016), security forces and academia often lag behind. Academic analyzes offer deep insights into radicalization, but their application is hampered by complexity and lack of practicality (Wall, 2007). This section explores two key reasons for this failure: overcomplicated narratives that fail to reach target groups and a lack of emotional engagement and simplicity in counterattacks.

Overcomplicated Narratives: Why Academic Analyzes Fail to Reach Target Groups

Extremist messages are quick and simple, like arrows aimed at vulnerable individuals (Malik, 2018). In contrast, academic analyzes often act as cumbersome nets that cannot capture the target (Desjardins, 2019). We can consider this through several aspects.

Unrecognizability and inaccessibility for target groups. The language of academic analysis is often too technical, full of theoretical concepts that are understandable only to a specialized audience (Europol, 2017). For example, sociological-cultural studies that see marginalization as a cause of radicalization use terms like "social capital" or "collective efficacy", which is far from the everyday experience of young people from vulnerable communities – the primary target of extremist messages (Wimmer, 2015). According to Wimmer, these groups require messages tailored to context, not abstract theories. The absence of simple language makes it impossible to directly influence individuals on the verge of radicalization.

Limited practical applicability. Theoretical frameworks often remain trapped in professional journals with a limited reach (Weimann, 2018). Even when they reach decision makers or practitioners on the ground, such as police officers or social workers, their complexity prevents implementation (Grabosky, 2017). A Europol report (2017) points out that practitioners do not have the capacity to decipher complex models, which creates a gap between theory and practice. According to Burton, while IS masterfully engages individuals, institutional responses lose ground due to over-academicization (Berton, 2015, as cited in Weimann, 2016).

Ignoring the local and cultural context. Academic analyzes often strive for universal solutions, ignoring local and cultural specificities (International Monetary Fund [IMF], n.d.). Extremism is deeply rooted in social context – a message that works in one community may be counterproductive in another (Wimmer, 2016). For example, analyzes that do not take into account ethnic tensions or religious sentiments in a particular region fail to get to the heart of the problem, making them less relevant to their target communities (Weimann, 2016).

Ignoring the influence of the digital world. In the digital era, extremists use social media, memes and viral messages to spread ideology, relying on brevity and emotion (Wimmer, 2016). Academic discourse, on the other hand, remains long and complex, hardly finding a place in this space where attention spans last eight seconds (Desjardins, 2019). Extremist content creates a sense of belonging, while academic works seem alienating, missing the opportunity to become part of a narrative that influences young people (Weimann, 2018).

Lack of interactivity. Academic publications are static and do not allow two-way communication (Wall, 2007). Target groups have questions and dilemmas that require interactivity, while extremists offer direct contact through platforms like Telegram (International Center for Counter-Terrorism [ICT], 2016). This lack of interaction further diminishes the impact of academic insights.

Lack of Emotional Engagement and Simplicity in Counterattacks

While extremists use emotions as weapons – fear, anger or pride – official counterattacks often remain sterile and devoid of force (Malik, 2018). One of the key problems of modern responses is the inability to emotionally engage the audience and simplify messages in an understandable and persuasive way.

The emotional void of the counter-narrative. Extremist messages reinforce a sense of belonging and identity, while counter-narratives ignore these emotional needs (Weimann, 2016). Institutional messages, such as "Terrorism destroys communities", rely on logic but do not touch the hearts of those whose radicalization begins with a sense of marginalization (Wimmer, 2016). A young person who feels alienated is not only looking for rational arguments, but also recognition of their emotions – which counter-narratives rarely provide (Weimann, 2018).

Complexity of messages and loss of attention. Extremists use concise slogans and short video clips that quickly attract attention (Malik, 2018). In contrast, counter-narratives often use technical language and long texts, losing competition in the digital world where attention is limited (Desjardins, 2019). Islamic State's message to "Be part of something bigger" fits into 140 characters, while institutional responses require paragraphs, making them unattractive.

Lack of authenticity. Extremist messages seem authentic because they speak directly to the experiences of the audience, often through community voices (Weimann, 2016). Counter-narratives from institutions are perceived as insincere or propaganda, especially due to the absence of local voices that would make them more believable (Malik, 2018).

Absence of cultural and local adaptation. Extremists use cultural references to increase influence, while counter-narratives remain generic and unadapted to the local context. A message adapted to Western society may be incomprehensible in collectivist cultures, which reduces its reach (Wimmer, 2016).

Focusing on punishment instead of prevention. Security responses often emphasize punishment – arrests and courts – to the neglect of empathy and prevention (Europol, 2017). This repression reinforces the sense of marginalization exploited by extremist, while positive preventive narratives are absent (Weimann, 2018).

Insufficient use of digital and creative tools. There are differences in the application of digital tools, with institutions tend to be quite conservative in this regard, while extremists use mimes and interactive formats (Weimann, 2016). This is also logical, bearing in mind that extremists want to increase the emotional reach of the counter-narrative, and this is achieved through creative approaches, e.g. short films or the inclusion of influencers (Malik, 2018).

What we usually have as answers is like fishing without the right bait – the answers are too complicated, without the emotional strength to successfully counter extremist narratives (IMF, n.d.). For a more effective fight against extremism, it is necessary to introduce simplicity, emotions and, necessarily, local context into the answers.

PROPOSING AN EFFECTIVE COUNTER-NARRATIVE

Extremist groups like IS have shown that they can successfully use Dak Net and social media for radicalization through simple and emotional narratives (Weimann, 2016). As we have stated, current responses suffer from overcomplication and lack of engagement, and an effective counter-narrative is expected to bridge this gap. It seems that the right solution could be to develop a strategy based on photos, videos and messages of up to 140 characters, which are, of course, adapted to the digital age and local contexts.

Why Simplicity Works: Psychology and Communication

Extremist messages work because they are concise and emotionally powerful, fostering a sense of belonging and purpose (Malik, 2018). As shown by some psychological studies, such messages require less cognitive effort, and this is also the reason why they reach the audience faster (Kahneman, 2011). Also, research shows that the optimal duration of attention in the digital space is eight seconds (Desjardins, 2019), and it is known in advance that complex narratives lose their impact. Therefore, the counter-narrative must be short and direct, with content from the everyday life of the target audience and, necessarily, with a positive message, which is also taken into account when creating extremist slogans.

Elements of a Successful Counter-Narrative: What to Include in 140 Characters

An effective counter-narrative should contain three key elements: emotion, authenticity and action. For example, a message like "Your voice changes the world - be part of the change" (103 characters) offers hope and inclusion, countering the extremist "Join the fight" (Malik, 2018). Photos of young people from local communities or short videos of successful reintegrations (Wimmer, 2016) reinforce the impression. These elements must be culturally adapted – what works in Indonesia may fail in the Middle East (Europol, 2017).

Examples: Specific Suggestions for Photos, Video Content and Short Messages

a) Photo: Picture of a group of young people building a park together, with the message "We are building the future together" (79 characters).

b) Video: 15-second clip about a former extremist who now runs a youth center, with the caption "My way is peace - find yours" (90 characters).

c) Message: "Your strength is in community, not in hatred" (107 characters), with a picture of a local festival.

These examples use visual power and brevity to convey a positive identity, countering extremist propaganda (Weimann, 2018). A counter-narrative of photos, videos

and 140 characters can rival extremist messages if it is simple, emotional and locally relevant (IMF, n.d.). This approach requires the cooperation of institutions, communities and digital experts in order to effectively counter radicalization.

IMPLEMENTATIONS AND CHALLENGES

A proposed counter-narrative based on photos, video and messages of up to 140 characters offers a simple and emotional response to extremism (Malik, 2018). However, its implementation requires strategic distribution and faces serious challenges. Therefore, it is necessary to consider how to reach the audience and overcome obstacles in practice.

Distribution Platforms: How to Reach an Audience on Social Media

The distribution of counter-narratives must take advantage of social networks such as TikTok, Instagram and Telegram, where extremists already operate (Weimann, 2016). Short video content and messages tailored to the algorithms of these platforms can quickly reach young people (Desjardins, 2019). For example, collaboration with local influencers on Instagram can increase the visibility of the message "Building the future together" (Wimmer, 2016). Institutions should hire digital marketing experts to ensure virality, while using paid campaigns to precisely target vulnerable groups (Europol, 2017). Quick adaptation to trends in the digital space is of great importance.

Potential Obstacles: Legal, Technical and Ethical Challenges

Implementation faces multiple obstacles. Legal challenges include regulation of privacy and data protection on platforms, such as GDPR in Europe, which can make it difficult to target audiences without breaking the law (Wall, 2007). In terms of technical challenges, they are seen in the rapid removal and adaptation of content by extremist groups. In order to achieve this, it is necessary to change sophisticated algorithms, that is, to carry out constant technological upgrading, for which advanced IT skills are necessary (Weimann, 2019). Ethical challenges concern the risk of stigmatizing communities if messages are misinterpreted as propaganda (IMF, n.d.). For example, a video about the reintegration of ex-extremists can cause negative reactions if it is not culturally sensitive (Wimmer, 2016). In addition, campaign financing and coordination between governments, NGOs and technology companies present logistical difficulties (Europol, 2017).

Effective implementation of counter-narratives requires smart distribution and overcoming legal, technical and ethical obstacles (Malik, 2018). Success depends on flexibility, cooperation and sensitivity towards local communities in order to counter extremist propaganda on their turf.

CONCLUSION

The connection of the digital world brings many good things into people's lives, but like many other human products whose primary purpose is the welfare of humanity, it has also brought some negative phenomena, among which is opening the door for extremism to take root in a way that was not possible before. The Dark Net and social media have become tools for terrorists to spread their messages, recruit followers and plan attacks, relying on simplicity that easily finds its way to vulnerable individuals. While they build their "theatre" online, security forces and academia remain stuck in a web of overanalysis and complex strategies that fail to reach where it is most needed – the ordinary people who are the targets of these messages. This paper shows that the crux of the problem lies precisely in this gap: while extremists use darts that hit the heart, the official responses are like fishing without the right bait - too convoluted to catch the right target.

Simplicity is what gives extremists an edge. Their messages don't require much thought - they are quick, clear and full of emotion that appeals to those who feel lost or rejected. On the other hand, institutions still offer answers that are far from everyday life, full of theories and technical concepts that do not speak the language of the communities they are intended for. Herein lies the key lesson: if we want to counter radicalization, we must fight on the same ground – the digital space where everything happens, and with tools that are as fast and powerful as those wielded by extremists. Photos, videos and messages of up to 140 characters are not just a technical gimmick, but a way to bring humanity back into the fight against hate, to show that community and hope can be stronger than fear and anger.

Implementing this approach is not an easy matter. Legal obstacles, such as privacy regulations, can slow down the process, while technological difficulties require constant monitoring and adaptation to the rapid changes introduced by extremists. Ethical challenges, such as the risk of stigmatization, remind us that every step must be carefully considered, because a wrong move can only deepen the gap between communities and institutions. Funding and coordination between different actors – governments, NGOs, technology companies – further complicate matters. But that's exactly where the strength of this proposal lies: it doesn't ask for a perfect system, but flexibility and a willingness to go where the people are, to speak their language and show them something they can believe in.

Ultimately, the fight against extremism is not only about security, but also about understanding. As long as the answers remain in offices and on the pages of thick reports, extremists will have the upper hand on the ground where the real battle is being fought - in the minds and hearts of individuals. The proposed counter-narrative is not a magic wand, but it is a step towards bringing that fight back to where it belongs: to the communities that can win it, given the chance. Simplicity, emotion and local context are not just tactics – they are a way to show that there is a better way, one that leads to togetherness, not destruction.

REFERENCE LIST

Berton, B. (2015, June). *The dark side of the web: ISIL's one-stop shop*. Report of the European Union Institute for Security Studies. The Dark Side of the Web: ISIL's One-Stop Shop?

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark web: A case study of Jihad on the web. *Journal of the American Society for Information Science and Technology*, 59(8), 134–1359. https://doi.org/ 10.1002/asi.20838

Europol. (2017). *Internet organised crime threat assessment (IOCTA)*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Grabosky, P. (2017). The evolution of cybercrime, 2006-2016. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 15–36). Routledge.

International Center for Counter-Terrorism [ICT]. (2016). *Trends in the Operational Arena*. https://www.jstor.org/stable/pdf/resrep09459.4.pdf

International Monetary Fund. (n.d.). The truth about the Dark Web. https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

International Telecommunication Union [ITU]. (2023, November 27). *New global connectivity data shows growth, but divides persist.* https://www.itu.int/en/mediacentre/Pages/PR-2023-11-27-facts-and-figures-measuring-digital-development.aspx

Jenkins, B. (1975). *International terrorism*. Crescent Publication.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Malik, N. (2018). T*error in the Dark.* Henry Jackson Society. https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Desjardins, J. (2019, March 13). *What happens in an Internet minute in 2019?* Visual Capitalist. https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Polity Press.

Weimann, G. (2016). Terrorist migration to the Dark Web. *Perspectives on Terrorism*, 10(3), 40–44. https://www.jstor.org/stable/26297596?seq=1

Weimann, G. (2018, April 27). *Going darker? The challenge of Dark Net terrorism.* Wilson Center. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf

Wimmer, A. (2016). *Dark net, social media and extremism: Addressing Indonesian counter-terrorism on the Internet*. Academia.edu. https://www.academia.edu/20813843/Dark_net_Social_Media_and_Extremism_Addressing_Indonesian_Counter_terrorism_on_the_Internet

Zirojević Fatić, M. (2011). Zloupotreba interneta u svrhe terorizma [Abuse of the Internet for terrorist purposes]. *Međunarodni problemi*, 63(3), 417–448.

Dijana Vučković[1]
Veselin Mićanović[2]

ETHICAL COMPETENCES FOR THE USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION

Abstract

Digital technology has brought numerous opportunities but also challenges in teaching and learning. Some of these challenges are particularly relevant in the context of preserving academic integrity. The rapid development of artificial intelligence further emphasizes the necessity of ethical education, as the opportunities available to students and other individuals in academia can be jeopardized if not used in an ethical manner. The Council of Europe, OECD, and UNESCO highlight the importance of the ethical dimension in education through their conventions and competency models for the use of artificial intelligence. The Council of Europe has published a convention focused on the protection of human rights in the era of artificial intelligence, UNESCO has developed competency models for teachers and students, and the OECD has produced various documents regulating the use of artificial intelligence. The goal of this work is to provide a comprehensive overview of the ethical dimension of education in the relevant reports, conventions, and competency models of the mentioned organizations. Our research question is: What ethical competencies are directly related to the use of artificial intelligence? We sought to answer this question using theoretical analysis, which includes a description of ethical competencies and their levels, with particular emphasis on UNESCO's competency models. Based on this analysis, we propose necessary implications for university teaching practice. In other words, based on the results of this desk research, we have created recommendations that could enhance the ethical component of teaching and learning in academia in the era of AI.

Keywords: *Academic Integrity, Ethical Competencies, Competency Models, Teacher, Artificial intelligence.*

INTRODUCTION

Artificial Intelligence (AI) represents the most important technological revolution of modern society. Its application in teaching, learning, and research, as well as in the entire academic sector, opens numerous opportunities for improving educational

1 Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, dijanav@ucg.ac.me
2 Faculty of Philosophy, University of Montenegro, Podgorica, Montenegro, veselinm@ucg.ac.me

and research processes. Furthermore, AI has capabilities that could certainly handle vast amounts of administrative tasks. AI is already present in many areas of education, from personalized learning that adapts to the needs of each student, thereby fulfilling the didactic principle of individualization like never before, to automated systems that assist in the analysis of large amounts of data.

Although AI brings numerous advantages and presents almost unimaginable possibilities, it must be kept in mind that its use also carries risks related to ethical dilemmas and data privacy issues. The development and application of AI in education is, therefore, not only a technological challenge, and it is not enough to simply train users for its use in this sense, but it is also an ethical issue, because each advancement requires a new level of responsibility. Academic integrity is a necessary prerequisite in the academic community, as its respect preserves the quality and reliability of the educational system, and aims to prevent the unethical use of technologies (Cotton, Cotton & Shipway, 2023). The implementation of AI must be subject to strict ethical standards that will ensure it is used in accordance with the values of the academic and wider social community, such as respect for human rights, justice, and integrity.

The goal of this paper is to analyze the ethical principles and competencies for using AI, which have been developed by organizations such as UNESCO, the Council of Europe, and the OECD. At the end of the paper, recommendations are provided that higher educational institutions (HEIs) can currently use for the safe and functional implementation of AI in teaching and learning processes.

OPPORTUNITIES AND ETHICAL DILEMMAS OF USING AI IN EDUCATION

AI and generative AI technology are rapidly developing and are recognized as key factors in transforming the education sector. The use of AI in teaching could dramatically improve the quality of education, allowing teachers to focus more on creative and interactive aspects of teaching, as well as on meaningful interactions with their students and colleagues, while AI takes on administrative tasks and provides personalized approaches to learning. However, AI also brings numerous challenges, and it is important to consider these when integrating AI into educational systems. In both academic and broader societal communities, there is a need to clearly define norms and guidelines for its responsible application.

OECD, reflecting on the potential ethical challenges of AI use, states:

> AI actors should respect the rule of law, human rights, democratic and human-centred values throughout the AI system lifecycle. These include non-discrimination and equality, freedom, dignity, autonomy of individuals, privacy and data protection, diversity, fairness, social justice, and internationally recognised labour rights.

> This also includes addressing misinformation and disinformation amplified by AI, while respecting freedom of expression and other rights and freedoms protected by applicable international law. To this end, AI actors should implement mechanisms and safeguards, such as capacity for human agency and oversight, including to address risks arising from uses outside of intended purpose, intentional misuse, or unintentional misuse in a manner appropriate to the context and consistent with the state of the art. (OECD, https://oecd.ai/en/dashboards/ai-principles/P6)

Therefore, it is evident that a human-centered approach and ethical use of AI must be prioritized, as otherwise, there is a risk of violating human rights and even undermining the fundamental principles of democracy itself.

Bit, Biwas and Nag (2024) explored the impact of artificial intelligence (AI) on education, highlighting its benefits and challenges. AI technologies such as natural language processing and machine learning can personalize learning, improve administrative efficiency, and increase student engagement. Benefits include tailored educational experiences, intelligent tutoring systems, data-driven insights, and increased accessibility for students with disabilities. AI also streamlines administrative tasks and supports collaboration between teachers and students. Challenges include concerns about privacy, potential biases, over-reliance on technology, cost differences, job loss, and ethical questions. A balanced approach is needed to maximize the benefits of AI while addressing these challenges (Bit, Biwas & Nag, 2024).

AI will certainly be applied in different ways across various fields of study. Below, we consider several potential general benefits that AI could bring to studies:

a. Improved Learning Experience through Personalization

AI enables personalized learning that adapts to the needs of each student (Feng, 2025). This concept essentially represents the fulfillment of the long-established principle of individualization in teaching, which didactics has never fully achieved. In the age of AI, by using intelligent tutoring systems and learning platforms, students can learn at their own pace, potentially increasing efficiency and motivation, although not necessarily, as social interaction and peer learning have important motivational benefits. Students with different learning styles can receive appropriate resources and support, enabling them to master the material in the best way.

b. Simplified Research Processes

AI-based tools such as Semantic Scholar allow researchers to more easily search and analyze literature (Razack et al., 2021). AI can shorten the time needed to study large amounts of academic papers. Moreover, AI can automatically summarize relevant information, helping researchers focus on the most important aspects of their research. This could potentially accelerate the discovery of new insights.

c. Fast and Efficient Data Analysis

In scientific disciplines that require, for example, statistics or any other large-scale data analysis, AI can process unimaginable amounts of data quickly (Ivanović, 2023). In the social sciences, for example, AI is used to analyze data from social networks and surveys, enabling a better understanding of public opinion and social changes. In educational research, AI can also process large amounts of data and, for instance, provide almost perfect learning analytics.

d. Enhanced Peer Review and Other Forms of Evaluation

AI plays a key role in the academic peer review process, where it can detect plagiarism, suggest reviewers, and even assess the quality of submitted papers. In teaching, following the same principle, AI can quickly and efficiently review students' work and provide valid and comprehensive feedback (Chang et al., 2023).

Given that AI can imitate human intelligence and process data faster and more accurately than humans, its potential in education is immense. For instance, AI can analyze student performance and difficulties in real-time, providing teachers with data that allows them to better tailor their teaching to each individual (Feng, 2025; Ivanović, 2023). Additionally, AI helps in self-regulating the learning process (Chang et al., 2023), as well as in evaluation and grading (Ding & Zou, 2024). However, the benefits of AI also come with significant challenges – ethical issues, data privacy concerns, and risks of over-reliance on technology that could reduce human creativity and critical thinking, meaning educational institutions must develop a balanced approach to AI usage (Cacho, 2024). Below are some identified risks:

a. Ethical Dilemmas

AI systems can express biases, even prejudices and stereotypes that exist in the data on which they are based (Ozkul, 2024; Zhou & Kawabata, 2023). For example, Ozkul (2024) points out that AI-produced technologies can produce discriminatory and biased results or analyses based on ethnicity, religion, and gender. Such biases towards certain social groups naturally raise concerns about fairness and transparency in AI use. Discrimination and bias in AI algorithms are based on the data used to train them, and this data may contain consciously or unconsciously produced prejudices or be biased. For example, if AI is used to select candidates for certain scholarships, the algorithm may unintentionally favor specific student groups based on data that does not reflect fairness (e.g., students from particular geographic areas, countries, ethnic groups, social classes, etc.). This type of bias can lead to increased inequality in educational systems and exacerbate existing social and economic differences.

The crucial question here is: According to which ethical norms and values does AI operate? In many cases, AI systems are developed in the context of specific

cultural and societal norms that may differ from those in educational systems of other countries. AI simply generates data collected from the internet, but not all societies participate equally in the production of internet content. For example, algorithms used to assess students, such as automated essay grading systems, may be insensitive to cultural differences in language and writing style, which can lead to inaccurate and unfair assessments. Or, if an algorithm uses pre-defined criteria that do not take into account creativity or originality, students who think outside the box may be unfairly graded. Additionally, it is important to consider how AI is used to create personalized learning experiences—whether the algorithms suggesting learning content are truly based on a general, balanced approach, or if they favor specific perspectives, strategies, techniques, and methodologies, thereby neglecting diversity in learning approaches.

b. Over-reliance on AI

If we become overly reliant on AI for grading or decision-making, it may result in reduced human creativity and critical thinking. While AI can automatically generate grades or decisions, the human factor in education is still crucial for understanding context and making moral decisions. Additionally, excessive reliance on AI can undermine students' ability to develop critical thinking and even their ability to learn through more complex forms of learning that depend on insight-based learning.

c. Privacy and Data Protection

AI systems that process sensitive data must comply with regulations regarding data protection. In the academic environment, where data about students, researchers, and teachers is processed, it is important to implement secure systems to prevent unauthorized access to data. The set of data collected in academic institutions may include information about students' abilities, learning preferences, grades, and other personal factors. Using this data to personalize learning can be useful, but it can also create opportunities for misuse. Furthermore, there are ethical concerns regarding data ownership – who owns the data that AI systems collect: students, educational institutions, or the companies that develop the AI technology?

d. Job Loss

The automation of administrative and teaching tasks may lead to job reductions, which raises concerns for many academic institutions. Institutions should invest in staff retraining to adapt to new technologies and ensure that jobs remain relevant in the AI era. One of the most concerning ethical challenges from the perspective of pedagogical-psychological and other educational sciences is the potential automation of educational processes, which could lead to reduced human engagement and, in some cases, even complete replacement of teachers by AI systems. From the perspective of educational sciences, this would make no sense, as social

constructivism, as the leading learning paradigm, clearly indicates that educational goals are far broader than cognitive learning outcomes, and issues related to the development of students' personalities in emotional, moral, social, etc., terms cannot be addressed without human interaction. AI can be an effective tool for administrative tasks in education, such as grading and tracking student progress, but it should not be considered as a replacement for teachers. Quality education is based on social and emotional interaction, which AI cannot provide. For instance, AI can analyze data about a student, but it cannot recognize the emotional or psychological needs of the student in the same way a teacher can.

Given the truly unprecedented opportunities that AI offers to universities for teaching and learning in the AI era, it is crucial to constantly be mindful of the ethical application of this advanced technology. Key areas requiring attention include data privacy protection, fairness in algorithm application, reducing human engagement to prevent job loss, and continuously updating appropriate ethical guidelines to ensure that AI is used in accordance with human rights and academic integrity principles.

ETHICAL DIMENSION OF AI USE IN RELEVANT INTERNATIONAL DOCUMENTS

EU Regulation 2024/1689 sets a framework for the ethical development and application of AI within the European Union. The goal of this document is to ensure transparent, fair, and responsible management of AI technologies, while respecting human rights and freedoms. AI systems created or used within the EU must comply with human rights, such as the right to privacy and freedom of expression, with an emphasis on preventing any discrimination or inequality among users, regardless of their personal and identity characteristics such as race, gender, or disability.

The leading principles of Regulation (Uredba, 2024) are transparency and accountability, implying that users and authorities must have a clear understanding of how AI systems operate and how they make decisions that affect their lives. Providers of AI systems should be held accountable for any misuse or errors the system may cause. Furthermore, the Regulation (2024) insists that human control must be present in all key decisions made by AI systems, especially concerning high-risk activities such as healthcare, justice, and employment.

User safety is, among other things, a priority, and AI systems, especially those that may present high risks, must undergo rigorous testing and certification to ensure their safety and prevent potential physical or mental harm to users. User privacy must be protected in accordance with data protection laws, and all data related to AI systems must be collected and processed legally.

Regulation (2024) also emphasizes social responsibility and sustainability, highlighting that AI technologies must contribute to positive social, economic, and ecological changes, rather than creating a wave of negative changes. It is important to ensure equal access to AI technologies for all EU citizens in order to prevent social inequality. The Regulation provides for continuous monitoring and revision of AI systems to ensure their alignment with ethical principles and appropriate laws.

The AI Act, discussed in March 2024 at the Plenary of the European Parliament (P9_TA(2024)0138 Artificial Intelligence Act), presents vital information for those involved in the development or application of AI technologies in the EU. This law aims to establish a regulatory framework that ensures the safety and protection of citizens while also encouraging innovation. The law is designed to minimize or completely eliminate the potential risks AI may pose to human rights and safety, while simultaneously enabling the competitiveness and development of this technological sector.

The law regulates all AI systems used within the EU and directs them towards a clear classification of potential risks. Based on this classification, AI systems that present a higher risk level are subject to strict regulations and enhanced oversight, while certain systems that pose unacceptable risks, such as biometric recognition in public spaces, are strictly prohibited. Providers of AI systems are responsible for product safety, and the law requires them to take measures for risk assessment and to enable monitoring of technology deployment. Transparency and the ability to audit AI systems are also mandatory (AI Act, 2024).

Although the law sets strict and sometimes rigorous rules, it simultaneously encourages innovation and competitiveness within the AI industry, aiming to position the European Union as a global leader in the responsible application of AI. For all providers and implementers of AI technologies, this document is crucial as it offers guidance on how to align their operations with legislation and ensure that AI systems are safe, ethically acceptable, and in compliance with legal norms.

The law particularly emphasizes the ethical aspects of AI application, including user rights protection and the prevention of discrimination. The goal is to ensure that AI systems do not infringe on human rights, such as privacy, freedom of speech, and the right to a fair trial. Within the law, ethical principles are key to shaping the legislative framework that will govern the development and application of AI in the EU. These principles aim to ensure that AI systems do not endanger the safety, freedoms, and rights of citizens but instead contribute to their well-being and positive social change.

The leading ethical principles of the AI Act by the European Commission (2024) are:

– Transparency and Accountability. Providers and users of AI systems must be able to clearly explain how their AI systems function, including an explanation of the methodology used. AI systems must also be designed in a way that enables accountability in the event of errors or harmful consequences.

– Ban on Discrimination. The AI Act has established frameworks to prevent any discrimination that AI systems might cause. The EU implements a policy of equality and non-discrimination, and all AI systems are expected not to make decisions that favor or discriminate against any individual or group based on race, gender, age, sexual orientation, disability, or other personal characteristics.
– Respect for Privacy and Data Protection. Since many AI systems use personal data to learn and make decisions, protecting privacy becomes crucial in the era of AI. The law is aligned with the General Data Protection Regulation (GDPR) and ensures that all AI technologies comply with the highest data protection standards.
– Human Control and Autonomy. The AI Act emphasizes human control in the decision-making process. Since AI can make decisions based on available data and algorithms, it is important that humans still have control over significant decisions, especially those that have a vital impact on people's lives.
– Safety and Security. AI systems must be designed in a way that does not jeopardize the physical and mental safety of users. For this reason, the law insists that all high-risk AI systems must undergo rigorous safety testing and that providers must continuously monitor system operations to detect potential problems in a timely manner.
– Access and Equality. The law also promotes inclusiveness in the application of AI technologies, ensuring equal access to AI for all EU citizens, who should have equal opportunities to use AI products and services.

These principles are not merely abstract guidelines but are concretely embedded in legislative regulations that define the obligations of providers, implementers, and end users of AI technologies. They are also foundational to building trust in AI technologies. They should enable individuals and society to trust that AI will contribute to positive changes without infringing on their fundamental rights and freedoms, and without posing a threat to safety.

The Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (Council of Europe, 2024), based on the Council of Europe's *Explanatory Report to the Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law* (2024), is a framework document that seeks to guide the development and application of artificial intelligence in Europe from an ethical standpoint, while respecting fundamental human rights, democracy, and the rule of law. Given that AI technology is increasingly shaping society, the Council of Europe considers it crucial to ensure that the use of AI systems complies with legislation that protects human welfare.

One of the key objectives of this Convention is the protection of human rights. This includes the right to privacy, freedom of speech, and the right to a fair trial, with a particular focus on ensuring that AI systems do not undermine any of these fundamental rights. In developing guidelines for the ethical use of AI, the Convention stresses that it

is necessary for AI technologies to operate in accordance with the fundamental values of society and to respect the integrity and safety of each individual.

Additionally, the Convention calls for transparency regarding how AI makes decisions. This means that users and authorities should have the ability to understand how AI systems function and based on which data decisions are made. This is particularly significant to avoid situations where people might be subjected to unjust or incomprehensible decisions made by AI systems.

The Council of Europe also highlights the importance of international cooperation among member states. Only through joint efforts and the exchange of best practices can global standards be created to ensure the responsible application of AI across various sectors, including education, healthcare, law, security, and the economy. Essentially, like documents created by the European Commission, this Convention seeks to balance technological progress with the preservation of human values, ensuring that AI is a technology or tool that contributes to the welfare of society rather than a threat to its foundations.

UNESCO'S COMPETENCY FRAMEWORKS FOR AI USE BY TEACHERS AND STUDENTS

UNESCO has played a key role in shaping a global ethical strategy for the use of AI, especially in education. They have developed guidelines and reference competency models focusing on how to use AI in a way that is safe, fair, beneficial for individuals, and society (UNESCO 2024a; 2024b). The key principles in UNESCO's models for AI usage include: the protection of human rights and dignity, access to education and reducing inequality, transparency and accountability, applying ethics in design and implementation, and AI education.

UNESCO's competency models for teachers and students (UNESCO 2024a; 2024b) offer educational guidelines based on understanding the ethical, social, and cultural aspects of using AI technologies. These models aim to balance technological progress with the need for responsible and ethical management of this technology. This is of particular importance for academic communities that wish to integrate AI into the teaching process. Essentially, students and teachers already use AI, but they do so without clear rules or limitations. Higher education institutions should adopt standards and guidelines for the responsible use of AI as early as possible (U.S. Department of Education, Office of Educational Technology, 2023). This also includes the development of competency models necessary for students, teachers, and researchers to use AI effectively.

The UNESCO AI Competence Frameworks for both teachers and students (2024a; 2024b) are clear, well-structured, and deeply thought-out documents created with the intent to provide guidelines on how AI can be integrated into teaching and learning.

What is particularly significant in this work is that both UNESCO models place a strong emphasis on ethical AI usage because "AI may threaten human agency, intensify climate change, violate data privacy, deepen long-standing systemic inequalities and exclusion, and lead to new forms of discrimination" (UNESCO, 2024b, p. 13).

UNESCO emphasizes that AI must inevitably be integrated into the communication between teachers and students, which it already is. This applies to all educational systems, although only a few have defined competencies or rules for AI usage. Both competency frameworks (for students and teachers) developed by UNESCO are based on the same methodological principles and have many common features, but they are not identical (UNESCO 2024a, 2024b). The framework for teachers covers 5 competency aspects defined across three levels of progression, making a total of 15 competency groups, while the framework for students also includes three levels of progression but for 4 aspects, totaling 12 groups. Two aspects have the same name in both frameworks: a human-centered approach and ethics of AI usage, but their specific competencies differ depending on whether the individual is a student or teacher (UNESCO 2024a, 2024b).

The aspect called Human-Centered Mindset is highlighted in both models, focusing on human agency and responsibility. (In addition to a human-centered approach, it might be suggested to add a nature-centered mindset, keeping in mind the principles of sustainable development). AI should be viewed as a technology that complements and helps accelerate human abilities rather than replaces or diminishes them. It is encouraging that UNESCO emphasizes this aspect, and according to the given models, both students and teachers should understand the implications of their interactions with AI and actively ensure that it serves humanity in ethical ways. Furthermore, "Values of empathy, altruism, justice, intercultural compassion and solidarity are essential for social cohesion and to uphold our common humanity. AI and other digital technologies must not discourage people from staying in contact with others and with the real world, as well as from respecting rights to ways of living and knowing beyond digital spaces" (UNESCO, 2024b, p. 16).

The aspect called Ethics of AI also appears in both UNESCO competency models. This aspect – which is directly related to the previous one – forms the core of the competency models (UNESCO 2024a; 2024b). Naturally, the elaboration of this aspect differs for teachers and students. For teachers, the focus is on creating a safe and responsible learning environment that includes AI technology, with the addition that teachers should contribute to the creation of ethical guidelines. Essentially, as AI advances, new ethical dilemmas will arise, making it particularly important for teachers to learn how to guide students through complex moral challenges. Therefore, teachers may experience a shift in their roles in an AI-driven learning environment, from being the content deliverer (a role AI might perform to some degree) to being those who focus on ethical principles and training students to respect those principles. Ethical principles such as data privacy, inclusivity, and sustainability are essential components for both students and teachers.

As already mentioned, the competencies are set at three proficiency levels (Table 1, Table 2). The first progression level in both models includes knowledge, skills, and attitudes related to artificial intelligence at a basic level, the second covers practical skills and the flexible application of AI, while the third level focuses on creating and evaluating content using AI. This hierarchical organization of levels is aligned with Bloom's taxonomy for the cognitive domain.

The competencies for teachers are defined across three levels of progression: acquisition, deepening, and creation (UNESCO 2024b).

Table 1. *Competency Framework for Teachers: Aspects and Levels of Progression*

Aspects	**Progression**		
	Acquire	Deepen	Create
Human-centered mindset	Human agency	Human accountability	Social responsibility
Ethics of AI	Ethical principles	Safe and responsible use	Co-creating ethical use
AI foundations and applications	Basic AI techniques and applications	Application skills	Creating with AI
AI pedagogy	AI-assisted teaching	AI-pedagogy integration	AI-enhanced pedagogical transformation
AI for professional development	AI enabling lifelong professional learning	AI to enhance organizational learning	AI to support professional transformation

Source: UNESCO AI competence framework for teachers (2024b, p. 22)

Five Aspects of Competencies for teachers are: Human-Centered Approach, AI Ethics, Fundamentals and Applications of AI, Pedagogy of AI, and AI for Professional Development (Table 1). These aspects are deeply interconnected, and each one has its own internal coherence. Each of them is formulated in terms of knowledge, skills, attitudes, and values as elements of learning and teaching. The ethical aspect, as already mentioned, emphasizes fundamental ethical principles, rules, institutional regulation, as well as practical ethical codes that teachers must adhere to. For teachers, this aspect involves progressing in understanding the ethical use of AI, skills for creating safe and responsible use of AI in an appropriate learning environment, as well as competencies necessary for developing and maintaining ethical norms (UNESCO, 2024b).

The first level (acquisition) of AI ethics for teachers involves having a deep understanding of ethical issues related to AI, as well as those encompassing the ethics of communication between humans and AI. This inevitably includes the protection of human rights, human agency, linguistic and cultural diversity, inclusive principles, and environmental protection (UNESCO, 2024b).

The second level (deepening) of ethical competencies for teachers relates to the safe and responsible use of AI in education. Teachers are expected to internalize ethical norms regarding safety and responsibility in the use of AI. These and other similar competencies must be an integral part of the norms across all phases of the educational process, including evaluation and assessment (UNESCO, 2024b).

The third level of this competency aspect for teachers focuses on updating and refining rules, which will be necessary due to the rapid development of AI technology. Thus, teachers' competencies are geared toward critical thinking, leading discussions, and activities related to ethical, sociocultural, and ecological issues. Given the rapid advancement of AI, it is expected that the process of updating ethical rules will be intense and continuous (UNESCO, 2024b).

The three levels of ethical development for teachers make sense because they ensure that teachers evolve with the technology. In addition to awareness of AI ethics, teachers should also be proactive when it comes to creating and enforcing those ethical boundaries.

Table 2. *AI competence framework for students*

Aspects	**Progression**		
	Understand	Apply	Create
Human-centered mindset	Human agency	Human accountability	Citizenship in the era of AI
Ethics of AI	Embodied ethics	Safe and responsible use	Ethics by design
AI techniques and applications	AI foundations	Application skills	Creating AI tools
AI system design	Problem scoping	Architecture design	Iteration and feedback loops

Source: UNESCO AI competence framework for students (2024a, p. 19)

The Ethical Aspect of AI for Students refers to the ethical judgments, reflections, and socio-emotional competencies that are necessary for students to understand, practically apply, and participate in adopting the rapidly growing normative framework for the use of AI. Students are expected to internalize ethics towards AI, which implies respecting human rights, justice, inclusion, equality, and other democratic values. Such ethics are based on the following principles: do no harm, proportionality in assessing AI use in a

given context, non-discrimination, sustainability, transparency and explainability, safe and responsible use, and ethics by design (UNESCO, 2024a). However, the cornerstone of safe AI use is "Critical thinking is a fundamental skill that students need to meaningfully engage with AI as learners, users and creators" (UNESCO, 2024a, p. 14).

The first level of competencies for students (understanding) refers to internalized ethics and implies that students can critically understand ethical issues related to AI, taking into account all the reference groups of concepts that need to be respected, such as human rights, justice, social equality, inclusion, climate change, etc. At this first level, the principles are: do no harm, proportionality, non-discrimination, human determination, and transparency (UNESCO, 2024a).

The second level, called safe and responsible use, relates to competencies that enable students to use AI responsibly. Students must also be aware of the existing risks associated with the use of AI, such as privacy protection risks. Additionally, students should be competent to take all necessary measures to ensure that their data is collected, shared, processed, and stored in ethically acceptable ways. At this level, the safety of student-users and their peers is also of significant importance (UNESCO, 2024a).

The third level (creation) relates to the competencies of creating and evaluating materials with the help of AI, as well as adopting and assessing regulations on AI.

The UNESCO competency frameworks complement the core principles of the Council of Europe's Convention (2024): respecting human dignity and individual autonomy, ensuring equality and non-discrimination, respecting privacy and the protection of personal data, enabling transparency and oversight, accountability, reliability, and ensuring safe innovations.

For students, the progression from embodied ethics to safe and responsible use to ethics by design is important because students need to internalize the ethical principles before they can apply them and eventually design systems in a responsible way.

Both frameworks align well with broader global principles outlined by organizations such as the Council of Europe and the OECD (2019; 2024). Principles such as human dignity, non-discrimination, and privacy protection are core to the ethical use of AI and ensuring its positive impact on society. This alignment shows UNESCO's commitment to ensuring that AI is not only effective in education but also contributes to social good and fairness.

These UNESCO frameworks provide a solid foundation for incorporating AI into educational systems. They not only address the technical and pedagogical aspects of AI but also emphasize the importance of ethics, human rights, and accountability, which are essential for ensuring that AI serves the public good. By promoting responsible AI use and developing ethical competencies among teachers and students, UNESCO is setting the stage for a future where AI enhances education while upholding key moral principles.

CONCLUSION AND RECOMMENDATIONS

Digital technologies, including the internet and AI, continuously raise new questions related to ethics and the responsible use of technology. In the context of education, ethical guidelines become even more important in order to preserve academic integrity. The use of AI in education should be guided by deep ethical principles, which include respect for human rights, data protection, and responsible use of technology. To prevent the misuse of AI, it is necessary to develop clear guidelines and regulations that will ensure that the technology is used in a way that contributes to the improvement of education, rather than diminishing its quality.

From the previous analyses, the need for constant oversight and updating of ethical guidelines is evident, as well as their incorporation into the ethical standards of higher education institutions. With the constant progress in the field of AI, educational institutions and policymakers must continually work on updating ethical codes and regulations related to the application of AI. For instance, as technology advances, new ethical insights must be developed, along with the updating of data privacy protection procedures and the fight against bias. Continuous updates to ethical guidelines must be based on an ongoing dialogue between teachers, students, decision-makers, and creators of educational policies and standards, as well as those who develop AI technologies.

The analysis of *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (U.S. Department of Education, Office of Educational Technology, 2023) points out that AI will undoubtedly influence the emergence of:

– Hybrid Learning Environments: AI will likely play a key role in the evolution of hybrid learning environments, where students can engage with materials both online and offline.
– Lifelong Learning: AI can support the trend toward lifelong learning by providing personalized education pathways for professionals who need to continuously update their skills in a rapidly changing job market.
– AI-powered Institutions: Some universities may even explore fully AI-powered or hybrid institutions that leverage AI to optimize teaching, learning, research, and administration.

All these guidelines, analyses, ideas, and current knowledge, which include assumptions for the future, must be accompanied by deep ethical reasoning based on respect for ethics and human rights. Therefore, competence models, such as those analyzed in this paper, must become an integral part of the regular training of teachers and students as soon as possible.

The analysis of *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (U.S. Department of Education, Office of Educational

Technology, 2023, p. 53–60) presents the following recommendations: Emphasize Humans in the Loop, Align AI Models to a Shared Vision for Education, Design Using Modern Learning Principles, Prioritize Strengthening Trust, Inform and Involve Educators, Focus R&D on Addressing Context and Enhancing Trust and Safety, and Develop Education-Specific Guidelines and Guardrails.

Thus, AI technologies are advancing at an extraordinary rate and are already being utilized by both teachers and students, often without clear guidelines and likely without deeper reflection on possible ethical dilemmas. It is clear that AI systems can offer a lot to the education sector; they can practically solve some issues that didactics has "dreamed" of for centuries but could not address in a traditional learning environment, such as issues related to individualization or personalized learning. In this sense, AI represents an opportunity that would likely enhance learning and research processes. However, the use of such sophisticated and powerful technology brings serious challenges, especially in the ethical domain. Therefore, it is reasonable to expect that higher education institutions will begin to develop guidelines for the use of AI in teaching, learning, and research, and that in these guidelines, a human and nature-centered mindset, along with AI ethics, will be dominant and pervasive principles.

REFERENCE LIST

Artificial Intelligence Act (2024). Regulation (EU) 2024/1689, *Official Journal of EU,* Brussels: European Union.

Bit, D., Biwas, S. & Nag, M. (2024). The Impact of Artificial Intelligence in Educational System. *International Journal of Scientific Research in Science and Technology*, 11(4), 419–427, https://doi.org/10.32628/IJSRST2411424

Cacho, R. (2024). Integrating Generative AI in University Teaching and Learning: A Model for Balanced Guidelines. *Online Learning*, 28(3), https://doi.org/10.24059/olj.v28i3.4508

Chang D. H., Lin M. P. C., Hajian S. & Wang Q. Q. (2023). Educational design principles of using AI chatbot that supports self-regulated learning in education: Goal setting, feedback, and personalization. *Sustainability*, 15(17), 12921. https://doi.org/10.3390/su151712921

Cotton, D. R. E., Cotton, P. A. & Shipway, J. R. (2023). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International,* 60(2), 228–239. https://doi.org/10.1080/14703297.2023.2190148

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024). Strasbourg, Council of Europe.

Ding L. & Zou D. (2024). Automated writing evaluation systems: A systematic review of grammarly, Pigai, and criterion with a perspective on future directions in the age of generative artificial intelligence. *Education and Information Technologies*, 29, 14151–14203. https://doi.org/10.1007/s10639-023-12402-3

Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, *Democracy and the Rule of Law* (2024). Strasbourg, Council of Europe.

Feng, L. (2025). Investigating the Effects of Artificial Intelligence-Assisted Language Learning Strategies on Cognitive Load and Learning Outcomes: A Comparative Study. *Journal of Educational Computing Research*, 62(8), 1961–1994. https://doi.org/10.1177/07356331241268349

Ivanović, I. (2023). Can AI-assisted Essay Assessment Support Teachers? A Cross-Sectional Mixed-Methods Reasearch Conducted at the University of Montenegro. *Annales – Series Historia et Sociologia*, 33(3), 571–590. https://doi.org/10.19233/ASHS.2023.30

OECD (2019). *AI Principles*. https://oecd.ai/en/dashboards/ai-principles/P6

OECD (2024). *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449

Ozkul, D. (2024). Artificial Intelligence and Ethnic, Religious, and Gender-Based Discrimination. *Social Inclusio*n, 12, Article 8942. https://doi.org/10.17645/si.8942

Razack H.I.A., Mathew S.T., Saad, F.F.A. & Alqahtani, S.A. (2021). Artificial intelligence-assisted tools for redefining the communication landscape of the scholarly world. *Science Editing*, 8(2), 134–144. https://doi.org/10.6087/kcse.244

U.S. Department of Education, Office of Educational Technology (2023). *Artificial Intelligence and Future of Teaching and Learning: Insights and Recommendations*. Washington, DC.

UNESCO (2024a). AI competency framework for students. Paris, UNESCO.

UNESCO (2024b). AI competency framework for teachers. Paris, UNESCO.

Uredba (EU) 2024/1689 Europskog Parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji). OJ EU 2024. Brussels: European Union.

Zhou, Y., & Kawabata, H. (2023). Eyes can tell: Assessment of implicit attitudes toward AI art. *I-Perception*, 14(5). https://doi.org/10.1177/20416695231209846

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.861(048)(0.034.4)
327.56:351.861(048)(0.034.4)

INTERNATIONAL Scientific Conference - BINS 2025 Transdisciplinarity of security studies and practice (2025 ; Belgrade)
Book of Abstracts [Електронски извор] / International Scientific Conference - BINS 2025 Transdisciplinarity of security studies and practice, Belgrade, May 8-9, 2025; [editor Milica Bošković]. - Belgrade : Faculty of Diplomacy and Security, 2025 (Belgrade : Faculty of Diplomacy and Security). - 1 електронски оптички диск (CD-ROM) : tekst ; 12 cm

Sistemski zahtevi: Nisu navedeni. - Tiraž 100.

ISBN 978-86-87545-49-6

а) Безбедност -- Међународни аспект -- Апстракти
б) Национална безбедност -- Апстракти
в) Безбедносни сектор -- Апстракти

COBISS.SR-ID 162889993
