Chapter 9

Ethical Use of Artificial Intelligence Applications in Early Childhood Education

Adem Yilmaz[1]

Mahmut Nacar[2]

Gülşah Uysal[3]

Abstract

The integration of Artificial Intelligence (AI) in education holds the potential to provide personalized learning and enhance educational experiences. However, it also raises significant concerns about data privacy and security, especially for young children who may not fully understand several aspects of data collection or usage practices. Protecting this data is of paramount importance. This text addresses ethical AI practices for safeguarding children's information, principles of data privacy, legal regulations, and the collaboration between parents and teachers. The use of AI in education must consider cultural sensitivities to accommodate diverse learner needs. Additionally, the discussion includes AI's potential risks, such as algorithmic bias, and strategies to mitigate these issues.

[1] Assoc. Prof. Dr., Kastamonu University Faculty of Education Department of Mathematics and Science Education, Science Education Division, yilmazadem@kastamonu.edu.tr, https://orcid.org/0000-0002-1424-8934

[2] PhD Student (Master's degree holder), Kastamonu University, Institute of Science, Department of Mathematics and Science Education, Science Education Division, mahmutnacar1984@gmail.com, https://orcid.org/0009-0008-2503-4393

[3] Master's degree holder, Ministry of National Education, Şanlıurfa Kırkmağara Middle School, Şanlıurfa/Türkiye, uysalgulsah@outlook.com, https://orcid.org/0009-0006-4825-0860

https://doi.org/10.58830/ozgur.pub534.c2203

1. The Importance of Ethics in AI for Early Childhood Education

1.1. Understanding Ethics in AI

1.1.1. Defining AI Ethics

Artificial Intelligence (AI) ethics refers to the moral guidelines and principles that govern the development and deployment of AI technologies. It encompasses a range of considerations, including fairness, transparency, accountability, privacy, and the overall impact on society (Jobin, Ienca & Vayena, 2019). AI ethics seeks to ensure that AI systems are designed and used in ways that respect human rights and promote well-being. In the context of early childhood education, AI ethics becomes particularly significant. Young children are in a critical stage of development, and the technologies they interact with can have profound effects on their cognitive, social, and emotional growth (Donohue & Schomburg, 2017). Therefore, integrating AI into early education requires careful ethical consideration to protect and nurture children's development.

1.1.2. Relevance to Early Childhood Education

AI technologies are increasingly being integrated into early childhood education settings. From interactive educational apps to AI-driven toys, these tools offer personalized learning experiences and can enhance engagement (Bers, 2018). However, without ethical oversight, they may also pose risks such as privacy invasion, bias reinforcement, or over-reliance on technology. Ethical considerations ensure that AI tools support educational goals without compromising children's rights or well-being (Zhu & Xie, 2019). This involves assessing the appropriateness of content, safeguarding personal data, and ensuring that AI interactions are developmentally suitable.

1.1.3. Ethical Principles in AI

Key ethical principles in AI include:

- **Beneficence**: AI should promote the well-being of users (Floridi et al., 2018).
- **Non-Maleficence**: AI should not cause harm.
- **Autonomy**: Respecting users' ability to make informed decisions.
- **Justice**: Ensuring fairness and equality in AI applications.
- **Explicability**: AI operations should be transparent and understandable.

Applying these principles in early childhood education ensures that AI tools are designed to benefit children, avoid harm, respect their emerging autonomy, promote fairness, and operate transparently.

1.1.4. Global Standards in AI Ethics

International bodies like UNESCO and the IEEE have proposed guidelines for ethical AI development (IEEE, 2019; UNESCO, 2019). These guidelines emphasize the importance of human rights, fairness, and transparency. For instance, UNESCO's Beijing Consensus highlights the need for AI in education to be inclusive and equitable. Adhering to global standards ensures consistency in ethical practices and protects children across different jurisdictions. It also fosters international collaboration in developing AI tools that meet high ethical standards.

1.2. The Role of Educators in Ethical AI Implementation

Educators are central to the ethical implementation of AI in early childhood education. Their roles include:

- **Ethical Awareness Among Educators**: Educators must understand the ethical implications of AI tools to make informed decisions about their use (Holmes et al., 2022).
- **Training for Responsible AI Use**: Professional development programs can equip educators with knowledge about AI ethics, data privacy, and appropriate pedagogical integration (Passey et al., 2018).
- **Guiding Children in Safe Technology Use**: Educators can teach children about responsible technology use, fostering digital literacy and ethical understanding from an early age (Livingstone & Blum-Ross, 2020).
- **Role of Institutions in Supporting Educators**: Schools and educational institutions should provide resources and support for educators, including policies and infrastructure that prioritize ethical AI use (Williamson & Eynon, 2020).

1.2.1. Case Studies on Educator-Led Ethical AI Use

Research indicates that when educators lead the ethical integration of AI, it results in:

- **Enhanced Learning Outcomes**: Thoughtful use of AI can personalize learning and address individual needs (Holmes et al., 2019).

- **Increased Ethical Awareness**: Educators can model ethical behavior and discuss ethical considerations with students, fostering critical thinking (Baker & Smith, 2019).
- **Community Engagement**: Involving parents and the community in discussions about AI use strengthens trust and collaboration.

1.3. Parental Concerns in AI Use

Parents play a crucial role in children's interactions with AI. Common concerns include:

- **Privacy and Data Security**: Worries about how children's data is collected, stored, and used (Chaudron et al., 2018).
- **Exposure to Inappropriate Content**: Fears that AI might expose children to content that is not age-appropriate.
- **Impact on Development**: Questions about how AI interactions might affect social skills, attention spans, and physical activity levels.

1.3.1. Privacy and Data Security for Children

Protecting children's personal data is a significant ethical issue. Regulations like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA) mandate strict controls over data collection and usage (European Commission, 2018; Federal Trade Commission, 2013). Ethical AI practices involve:

- **Data Minimization**: Collecting only the data necessary for functionality.
- **Transparency**: Clearly informing parents about data practices.
- **Security Measures**: Implementing robust protection against data breaches.

1.3.2. Parents' Role in AI Ethical Education

Parents can support ethical AI use by:

- **Engaging in Open Dialogue**: Discussing technology use with their children and setting appropriate boundaries (Livingstone & Byrne, 2018).
- **Educating Themselves**: Staying informed about AI technologies and their implications.

- **Collaborative Approaches with Schools**: Working with educators to ensure consistent practices between home and school.

1.3.3. Addressing Parental Misinformation on AI

There is a need to address misconceptions about AI. Providing accurate information through:

- **Workshops and Seminars**: Educational sessions for parents.
- **Resource Materials**: Guides and fact sheets explaining AI in accessible language.
- **Communication Channels**: Regular updates from schools about AI initiatives.

1.4. Ethics in AI: Cultural Sensitivity in Early Childhood

1.4.1. Cultural Factors in Ethical AI Use

Cultural context influences how AI is perceived and utilized. Ethical AI must consider:

- **Language Diversity**: Supporting multiple languages to be inclusive.
- **Cultural Norms and Values**: Respecting different beliefs and practices.
- **Representation**: Ensuring diverse cultural backgrounds are represented in AI content.

1.4.2. Diversity and Inclusion in AI Tools

Inclusive AI design involves:

- **Avoiding Bias**: Ensuring algorithms do not favor certain groups over others (Mehrabi et al., 2021).
- **Culturally Relevant Content**: Providing materials that reflect the backgrounds of all students.
- **Accessibility**: Designing for children with different abilities and needs.

1.4.3. Addressing Cultural Bias in AI Algorithms

Bias in AI can reinforce stereotypes or exclude certain groups. Mitigating bias involves:

- **Diverse Data Sets**: Training AI on data that represents a wide range of populations.
- **Algorithm Audits**: Regularly checking AI outputs for bias.
- **Stakeholder Involvement**: Including input from various cultural groups in development.

1.4.4. Promoting Multicultural Awareness

AI can be a tool to:

- **Enhance Cultural Understanding**: Exposing children to different cultures through interactive experiences.
- **Support Language Learning**: Offering multilingual options.
- **Foster Inclusion**: Creating collaborative activities that celebrate diversity.

1.4.5. Case Studies on Culturally Sensitive AI

Successful implementations demonstrate:

- **Improved Engagement**: Children engage more with content that reflects their identity (Santos et al., 2016).
- **Positive Social Outcomes**: Inclusive AI promotes empathy and reduces prejudice.

1.5. Future Perspectives in Ethical AI Education for Children

1.5.1. Emerging Ethical Challenges in AI

As AI evolves, new challenges arise:

- **Deepfakes and Misinformation**: Potential for AI to create realistic but false content.
- **Autonomy and Agency**: Balancing AI assistance with encouraging independent thinking.
- **Emotional AI**: AI that reads or responds to emotions raises privacy concerns.

1.5.2. Preparing Children for Future AI Interactions

Education should:

- **Develop Critical Thinking**: Teach children to question and analyze AI outputs.
- **Promote Ethical Reasoning**: Encourage discussions about right and wrong in technology use.
- **Enhance Digital Literacy**: Equip children with skills to navigate a tech-rich world.

1.5.3. Ethical Curriculum Development

Integrating ethics into curricula involves:

- **Interdisciplinary Approaches**: Combining technology education with social sciences and humanities.
- **Active Learning**: Using projects and discussions to explore ethical issues.
- **Assessment of Ethical Understanding**: Evaluating students' grasp of ethical concepts.

1.5.4. Role of Policy in Shaping Future AI Ethics

Policies can:

- **Set Standards**: Establish clear guidelines for AI use in education.
- **Provide Resources**: Fund initiatives that promote ethical AI.
- **Facilitate Collaboration**: Encourage partnerships between educators, technologists, and policymakers.

1.5.5. Encouraging Ethical Mindsets Early On

Fostering ethics in early childhood lays the foundation for responsible citizenship. Strategies include:

- **Modeling Ethical Behavior**: Adults demonstrating integrity and respect.
- **Creating Ethical Environments**: Classrooms that value fairness and empathy.
- **Empowering Children**: Involving them in decision-making processes.

The provided section offers a comprehensive exploration of the critical role that ethics plays in integrating Artificial Intelligence (AI) into early childhood education. It systematically addresses the definition of AI ethics, its relevance to young learners, ethical principles, global standards, the roles of educators and parents, cultural sensitivity, and future ethical challenges. This evaluation aims to analyze the strengths of the section and suggest areas for enhancement, supported by relevant academic literature.

The section begins by defining AI ethics as the moral guidelines and principles that govern the development and deployment of AI technologies, emphasizing considerations such as fairness, transparency, accountability, privacy, and societal impact (Jobin et al., 2019). This foundational explanation is crucial as it sets the context for the ethical discourse surrounding AI. By highlighting the profound effects that AI technologies can have on children's cognitive, social, and emotional development (Donohue & Schomburg, 2017), the section underscores the necessity of ethical considerations when integrating AI into early education.

The increasing integration of AI technologies in early childhood settings, such as interactive educational apps and AI-driven toys, offers personalized learning experiences and enhanced engagement (Bers, 2018). However, the section rightly points out the potential risks without ethical oversight, including privacy invasion, bias reinforcement, and over-reliance on technology (Zhu & Xie, 2019). This balanced perspective acknowledges both the benefits and drawbacks of AI in education, aligning with current academic discussions on the responsible use of technology in learning environments (Holmes et al., 2022).

The enumeration of key ethical principles—beneficence, non-maleficence, autonomy, justice, and explicability—is well-articulated (Floridi et al., 2018). Applying these principles to early childhood education ensures that AI tools are designed to benefit children, avoid harm, respect their emerging autonomy, promote fairness, and operate transparently. This approach aligns with ethical frameworks proposed by leading scholars and organizations, emphasizing the importance of human-centered AI (Floridi & Cowls, 2019).

By referencing global standards set by organizations like UNESCO and the IEEE (IEEE, 2019; UNESCO, 2019), the section effectively situates the discussion within an international context. The mention of UNESCO's Beijing Consensus highlights the global commitment to inclusive and equitable AI in education. This emphasis on adhering to international guidelines ensures consistency in ethical practices and protects children across different jurisdictions. It also fosters international collaboration in developing AI tools that meet high ethical standards (Jobin et al., 2019).

The section appropriately identifies educators as central figures in the ethical implementation of AI in early childhood education. It outlines their roles in fostering ethical awareness, receiving training for responsible AI use, guiding children in safe technology practices, and being supported by institutions (Aksoy & Küçük Demir, 2019; Ayyıldız & Yılmaz, 2021; Holmes et al., 2022). This aligns with research that underscores the importance of teacher professional development in technology use (Passey et al., 2018). By equipping educators with the necessary knowledge and skills, they can make informed decisions and model ethical behavior, thereby fostering critical thinking among students (Baker & Smith, 2019).

The inclusion of research indicating positive outcomes when educators lead ethical AI integration adds credibility. The mention of enhanced learning outcomes, increased ethical awareness, and community engagement demonstrates the multifaceted benefits of educator-led initiatives (Holmes et al., 2019; Yılmaz, Şahin-Atılgan & Güzel-Sekecek, 2024). However, the section could be strengthened by providing specific examples or studies that detail these results, offering concrete evidence of the impact of such practices.

Acknowledging the crucial role of parents, the section addresses common concerns such as privacy, data security, exposure to inappropriate content, and the impact on development (Chaudron et al., 2018). By highlighting these issues, the section emphasizes the need for transparency and collaboration between schools and families. The reference to regulations like the GDPR and COPPA (European Commission, 2018; Federal Trade Commission, 2013) underscores the legal imperatives for protecting children's personal data.

The discussion on ethical AI practices involving data minimization, transparency, and security measures is timely and relevant. With increasing awareness of data privacy issues, particularly in education, these practices are essential for safeguarding children's information (Livingstone & Blum-Ross, 2020). The section effectively connects ethical principles with practical measures, promoting responsible data handling.

Encouraging parents to engage in open dialogue, educate themselves, and collaborate with schools reflects best practices in digital parenting (Livingstone & Byrne, 2018). The section recognizes that parents' involvement is pivotal in ensuring consistent practices between home and school, which can enhance children's understanding and responsible use of AI technologies.

The suggestion to provide accurate information through workshops, resource materials, and communication channels is proactive. Misinformation can lead to unwarranted fears or misuse of technology. By equipping parents with knowledge, schools can build trust and facilitate a supportive environment for integrating AI ethically (Livingstone & Blum-Ross, 2020).

The section's focus on cultural factors in ethical AI use is commendable. It highlights the importance of language diversity, respecting cultural norms and values, and ensuring representation in AI content. This aligns with the principles of inclusive education and addresses concerns about bias and fairness in AI systems (Mehrabi et al., 2021; Yılmaz, Uysal & Nacar, 2024).

By discussing inclusive AI design—avoiding bias, providing culturally relevant content, and ensuring accessibility—the section underscores the need for AI tools that cater to diverse learners. This approach supports educational equity and can contribute to reducing disparities in educational outcomes (Chen & Li, 2010; Öztürk, 2023).

The acknowledgment of bias in AI algorithms and strategies to mitigate it, such as using diverse data sets and conducting algorithm audits, is critical. Bias in AI can perpetuate stereotypes and systemic inequalities (Buolamwini & Gebru, 2018). The emphasis on stakeholder involvement ensures that multiple perspectives are considered, enhancing the fairness and accuracy of AI applications.

The section suggests that AI can enhance cultural understanding, support language learning, and foster inclusion. These applications of AI can enrich the educational experience and promote social cohesion. By providing interactive and engaging content, AI tools can expose children to different cultures, fostering empathy and global awareness (Santos et al., 2016).

Identifying emerging ethical challenges such as deepfakes, autonomy, and emotional AI reflects an awareness of the rapidly evolving AI landscape. Preparing children for future AI interactions by developing critical thinking, ethical reasoning, and digital literacy is essential (Long & Magerko, 2020). This proactive approach equips children with the skills needed to navigate complex technological environments responsibly.

Integrating ethics into curricula through interdisciplinary approaches, active learning, and assessment aligns with contemporary educational strategies (Gašević et al., 2015; Yılmaz, Gülgün, Çetinkaya & Doğanay, 2018). By embedding ethical considerations into learning experiences, educators can cultivate ethical mindsets and promote lifelong ethical awareness.

The section appropriately highlights the role of policy in setting standards, providing resources, and facilitating collaboration. Policies can drive systemic change and ensure that ethical considerations are embedded at all levels of education (Selwyn & Gašević, 2020). Encouraging partnerships among educators, technologists, and policymakers can foster a holistic approach to ethical AI integration.

The emphasis on modeling ethical behavior, creating ethical environments, and empowering children is aligned with theories of moral development and ethical education (Kidron & Rudkin, 2020). By instilling ethical values early, educators and parents can lay the foundation for responsible citizenship and ethical decision-making in the digital age.

The section provides a thorough examination of the importance of ethics in AI for early childhood education, integrating theoretical concepts with practical applications. It effectively addresses the multifaceted nature of ethical considerations, from individual interactions to global standards. To enhance the section further, incorporating empirical studies or specific examples of successful implementations could provide stronger evidence of the concepts discussed. Additionally, exploring potential challenges in implementing ethical AI practices, such as resource constraints or resistance to change, could offer a more nuanced perspective.

2. Privacy and Security in AI for Early Childhood Education

The integration of Artificial Intelligence (AI) in early childhood education offers significant opportunities for personalized learning and enhanced educational experiences. However, it also raises critical concerns regarding privacy and security, particularly when it involves young children who are less capable of understanding and consenting to data collection and use practices. This section explores the multifaceted issues surrounding privacy and security in AI applications for early childhood education, emphasizing the importance of protecting children's data, implementing robust cybersecurity measures, balancing personalization with privacy, and fostering collaboration between parents and educators.

2.1. Children's Data Privacy Concerns

2.1.1. Understanding Data Privacy for Children

In the digital age, data has become a valuable commodity, and the education sector is no exception. AI systems in education often rely on collecting and analyzing data to tailor learning experiences to individual students (Ayyıldız, Yılmaz & Baltacı, 2021; Holmes et al., 2019). When dealing with young children, data privacy concerns become more pronounced due to their vulnerability and limited capacity to comprehend the implications of data sharing. Children's data can include personal identifiers, learning behaviors, emotional responses, and even biometric information collected through AI-enabled devices (Livingstone & Stoilova, 2021). This sensitive information, if mishandled, can lead to serious consequences such as identity theft, profiling, or unauthorized surveillance.

Protecting children's data privacy is crucial for several reasons:

- **Legal and Ethical Obligations**: There are stringent laws and ethical guidelines governing the collection and use of children's data, recognizing their inability to provide informed consent (European Commission, 2018).
- **Psychological Well-being**: Infringements on privacy can affect a child's sense of security and trust in educational institutions (Barth & de Jong, 2017).
- **Long-term Implications**: Data collected during childhood can have lasting effects, influencing future opportunities and personal development if not properly safeguarded (Lievens et al., 2018).

2.1.2. Legal Regulations on Children's Data

Several international and national regulations have been established to protect children's data privacy. Notably:

- **General Data Protection Regulation (GDPR)**: Implemented by the European Union, GDPR sets strict rules for data processing, requiring parental consent for children under 16 and emphasizing transparency and the right to be forgotten (European Commission, 2018).
- **Children's Online Privacy Protection Act (COPPA)**: In the United States, COPPA imposes requirements on online services aimed at children under 13, mandating parental consent and clear privacy policies (Federal Trade Commission, 2013).
- **United Nations Convention on the Rights of the Child (UNCRC)**: Provides a global framework recognizing children's rights to privacy and protection from exploitation (United Nations, 1989).

These regulations highlight the necessity for educational institutions and AI developers to comply with legal standards, ensuring that data collection practices are lawful, transparent, and respectful of children's rights.

2.1.3. Risks of Data Collection in AI Tools

AI tools often require extensive data to function effectively, which can pose several risks:

- **Data Breaches**: Unauthorized access to databases can expose sensitive information, leading to identity theft or other malicious activities (Ponemon Institute, 2019).
- **Misuse of Data**: Collected data might be used for unintended purposes, such as targeted advertising or profiling, without parental knowledge or consent (Zhao et al., 2019).
- **Surveillance and Autonomy**: Excessive monitoring can infringe on children's autonomy and create a culture of surveillance, affecting their development and behavior (Taylor & Rooney, 2017).

To mitigate these risks, it's essential to limit data collection to what is necessary, implement strong security measures, and ensure transparency with parents and guardians.

2.2. Importance of Parental Consent

Parental consent is a critical component in safeguarding children's data privacy. It involves:

- **Informed Consent**: Providing clear, accessible information to parents about what data is collected, how it will be used, and who will have access to it (van der Hof, 2016).
- **Opt-in Mechanisms**: Default settings should favor privacy, requiring active consent from parents rather than passive acceptance (Nemorin, 2017).
- **Continuous Communication**: Keeping parents informed about any changes in data practices or breaches, fostering trust and collaboration.

By actively involving parents, educational institutions can ensure compliance with legal requirements and reinforce ethical practices.

2.2.1. Data Privacy Education for Parents and Educators

Education plays a vital role in enhancing data privacy. Parents and educators should be informed about:

- **Data Privacy Principles**: Understanding concepts like data minimization, purpose limitation, and rights to access and erasure (ICO, 2018).

- **Risks and Threats**: Recognizing potential dangers associated with data collection and AI technologies (Livingstone et al., 2018).
- **Best Practices**: Implementing strategies to protect data, such as secure passwords, cautious sharing, and regular updates (Stoilova et al., 2020).

Workshops, seminars, and resource materials can empower parents and educators to take proactive steps in protecting children's data.

2.2.2. Common Security Risks in AI Systems

AI systems in education face several cybersecurity threats:

- **Malware and Ransomware**: Malicious software can infiltrate systems, encrypt data, and demand payment for its release (Huang & Zhu, 2019).
- **Phishing Attacks**: Deceptive communications aiming to trick users into revealing sensitive information (Jansen & van Schaik, 2019).
- **Insider Threats**: Unauthorized access or misuse of data by individuals within the organization (Schneider et al., 2015).

These risks necessitate robust cybersecurity strategies to protect sensitive data and maintain the integrity of educational systems.

2.3. Protecting Early Childhood Data from Breaches

Key measures to safeguard data include:

- **Encryption**: Encoding data to prevent unauthorized access during transmission and storage (Almohri et al., 2016).
- **Access Controls**: Implementing role-based access to limit who can view or modify data (Ferreira et al., 2014).
- **Regular Audits and Monitoring**: Continuously assessing systems for vulnerabilities and unusual activities (Kallberg, 2016).
- **Incident Response Plans**: Establishing protocols to respond swiftly to breaches, minimizing damage and restoring security (NIST, 2018).

Implementing these measures helps protect children's data and reinforces trust in AI-based educational tools.

2.4. Role of IT in Ensuring AI Security

Information Technology (IT) departments play a pivotal role by:

- **Designing Secure Systems**: Integrating security into the architecture of AI systems from the outset (Bishop, 2018).
- **Implementing Updates and Patches**: Keeping software current to address known vulnerabilities (Alqahtani et al., 2019).
- **Training Staff**: Educating educators and administrators on security protocols and best practices (Wilson & Hash, 2003).
- **Collaborating with Stakeholders**: Working with developers, educators, and policymakers to align security measures with educational goals.

Effective IT management ensures that security is an integral part of AI implementation in education.

2.5. Educator's Role in Cybersecurity Awareness

Educators contribute to cybersecurity by:

- **Modeling Responsible Behavior**: Demonstrating proper use of technology and adherence to security protocols (Johnson et al., 2016).
- **Teaching Digital Literacy**: Incorporating cybersecurity education into the curriculum, empowering students to protect themselves (Huang et al., 2020).
- **Reporting Issues**: Identifying and reporting suspicious activities or potential threats to IT departments promptly.

Their engagement enhances the overall security posture and promotes a culture of vigilance.

2.5.1. Case Examples of Security Breaches

- **Edmodo Breach (2017)**: A massive data breach exposed millions of user accounts due to inadequate security measures, highlighting the vulnerability of educational platforms (Cimpanu, 2017).
- **UK School Ransomware Attack (2019)**: Cybercriminals targeted a school's network, disrupting operations and emphasizing the need for robust cybersecurity defenses (BBC News, 2019).

These cases illustrate the real-world consequences of security lapses and the importance of proactive measures.

2.6. Benefits of Personalized Learning

Personalized learning through AI offers:

- **Customized Content**: Adapting lessons to individual learning styles and paces (Pane et al., 2015).
- **Improved Engagement**: Increasing motivation by aligning materials with students' interests and needs (Walkington, 2013).
- **Data-Driven Insights**: Providing educators with valuable information to support student development (Daniel, 2015).

2.6.1. Risks of Over-Personalization

However, over-personalization can lead to:

- **Privacy Intrusions**: Excessive data collection infringing on personal privacy (Regan & Jesse, 2019).
- **Algorithmic Bias**: AI systems reinforcing existing biases, leading to unfair treatment (Noble, 2018).
- **Reduced Exposure**: Limiting students' exposure to diverse ideas and challenges by tailoring content too narrowly (Selwyn, 2019).

It's crucial to find a balance that leverages personalization benefits without compromising privacy or educational breadth.

2.6.2. Ethical Boundaries of Data Usage

Establishing ethical boundaries involves:

- **Transparency**: Clearly communicating data practices to students and parents (Floridi, 2016).
- **Consent and Control**: Allowing users to consent to data collection and control how their data is used (Solove, 2013).
- **Purpose Limitation**: Using data solely for educational purposes and not for commercial exploitation (Wachter et al., 2017).
- **Accountability**: Implementing oversight mechanisms to ensure compliance with ethical standards (Mittelstadt et al., 2016).

By adhering to these principles, educators and developers can use data responsibly.

2.7. Minimizing Data Collection in AI

Strategies include:

- **Data Minimization**: Collecting only data essential for functionality (Cavoukian, 2011).

- **Anonymization and Pseudonymization**: Removing identifiable information to protect privacy (El Emam & Arbuckle, 2013).
- **Local Processing**: Keeping data on local devices rather than transmitting it to central servers (McMahan & Ramage, 2017).

These approaches reduce privacy risks while maintaining the effectiveness of AI tools.

2.8. Transparency with Personalization Techniques

Ensuring transparency involves:

- **Explainable AI**: Designing systems that can explain how decisions are made (Gunning, 2017).
- **User Education**: Informing users about how personalization works and its implications (Abdul et al., 2018).
- **Feedback Mechanisms**: Allowing users to correct or challenge AI-generated recommendations (Ananny & Crawford, 2018).

Transparency builds trust and empowers users to engage with AI technologies confidently.

Parental and Educator Collaboration on Security

2.9. Joint Efforts in Child Data Protection

Collaboration enhances security by:

- **Sharing Knowledge**: Parents and educators exchanging information about risks and best practices (Livingstone & Haddon, 2009).
- **Coordinated Policies**: Aligning rules and guidelines across home and school environments (Powers & Green, 2018).
- **Support Networks**: Creating communities that support each other in safeguarding children (Zilka, 2017).

2.9.1. Developing Privacy Policies with Parents

Involving parents in policy development:

- **Increases Relevance**: Policies reflect the concerns and values of the community (Shapiro & Stefkovich, 2016).
- **Enhances Compliance**: Parents are more likely to support and adhere to policies they helped create (Epstein et al., 2018).

- **Fosters Trust**: Collaborative processes build stronger relationships between schools and families.

2.9.2. Regular Security Audits in Schools

Audits help maintain security by:

- **Identifying Gaps**: Revealing weaknesses in systems and processes (Safa et al., 2016).
- **Updating Practices**: Ensuring that security measures keep pace with evolving threats (Ashford, 2017).
- **Demonstrating Commitment**: Showing stakeholders that the institution prioritizes security.

2.9.3. Educator Training on Data Security

Training programs should:

- **Provide Practical Skills**: Teach educators how to implement security measures effectively (Johnson, 2012).
- **Update Knowledge**: Keep staff informed about the latest threats and technologies (Alshammari & Singh, 2018).
- **Promote a Security Culture**: Encourage proactive attitudes toward data protection.

2.9.4. Community Forums on AI Safety

Forums can:

- **Raise Awareness**: Educate the community about AI and associated risks (Hassani et al., 2018).
- **Encourage Dialogue**: Facilitate discussions between stakeholders (Feenberg & Bakardjieva, 2004).
- **Develop Solutions**: Collaboratively address challenges and share best practices.

These collaborative efforts strengthen the overall security framework and promote responsible AI use. The provided section offers a comprehensive exploration of the multifaceted issues surrounding privacy and security in the integration of Artificial Intelligence (AI) into early childhood education. It delves into the critical concerns of children's data privacy, the importance of parental consent, cybersecurity risks, and the collaborative roles of educators and parents. This evaluation aims to analyze the key themes presented, assess their relevance and alignment with current academic discourse, and suggest areas for further enhancement. The section begins by highlighting the growing value of data in the digital age and its implications for the education sector (Bellman, 1978; Holmes et al., 2019; Yılmaz & Salman, 2022). It astutely recognizes that young children are particularly vulnerable due to their limited understanding of data sharing implications (Livingstone & Stoilova, 2021). The emphasis on the sensitivity of children's data—including personal identifiers, learning behaviors, emotional responses, and biometric information—is timely and significant. Mishandling such data can lead to severe consequences like identity theft, profiling, or unauthorized surveillance (Aydoğdu et al., 2019; Barth & de Jong, 2017). The discussion on legal and ethical obligations, psychological well-being, and long-term implications underscores the necessity of stringent data protection measures. References to international regulations like the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA) reinforce the global importance of these concerns (European Commission, 2018; Federal Trade Commission, 2013). This alignment with legal frameworks adds credibility and context to the argument.

The section effectively underscores parental consent as a critical component in safeguarding children's data privacy. By detailing elements such as informed consent, opt-in mechanisms, and continuous communication, it emphasizes the need for transparency and active parental involvement (Nemorin, 2017; van der Hof, 2016). This approach is consistent with best practices in data protection, recognizing parents as key stakeholders in their children's digital experiences.

Highlighting the role of education in enhancing data privacy awareness is a strong point. By advocating for informing parents and educators about data privacy principles, risks, threats, and best practices, the section promotes proactive engagement (ICO, 2018; Yılmaz, 2021a). This strategy is essential in fostering a culture of vigilance and responsibility among those directly involved with children's education and technology use.

The enumeration of cybersecurity threats such as malware, ransomware, phishing attacks, and insider threats provides a realistic portrayal of the challenges faced by AI systems in education (Huang & Zhu, 2019; Jansen & van Schaik, 2019; Schneider et al., 2015). By identifying these risks, the section sets the stage for discussing robust cybersecurity strategies, emphasizing the need for a comprehensive approach to protect sensitive data and maintain system integrity.

The proposed measures i.e., encryption, access controls, regular audits and monitoring, and incident response plans are practical and align with established cybersecurity practices (Almohri et al., 2016; Kallberg, 2016; NIST, 2018). Emphasizing these technical safeguards demonstrates an understanding that data protection requires both policy and technical solutions. The integration of these measures helps build trust in AI-based educational tools, which is crucial for their acceptance and effectiveness.

Acknowledging the pivotal role of Information Technology (IT) departments adds depth to the discussion. By outlining responsibilities such as designing secure systems, implementing updates and patches, training staff, and collaborating with stakeholders, the section highlights the multifaceted efforts required to ensure AI security (Alqahtani et al., 2019; Bishop, 2018). This comprehensive view reinforces the idea that security is not solely a technical issue but also an organizational one that necessitates coordination across various domains.

The section aptly identifies educators as key players in promoting cybersecurity. By modeling responsible behavior, teaching digital literacy, and reporting issues, educators contribute to a culture of vigilance and safety (Huang et al., 2020; Johnson et al., 2016). This aligns with current research emphasizing the importance of incorporating cybersecurity education into the curriculum to empower students (Öztürk & Demiroğlu Çiçek, 2024; Tisdale, 2015).

Inclusion of real-world examples such as the Edmodo breach (2017) and the UK school ransomware attack (2019) adds practical significance to the discussion (BBC News, 2019; Cimpanu, 2017; Sevgi, Ayyıldız & Yılmaz, 2023). These cases illustrate the tangible consequences of inadequate security measures and underscore the urgency for proactive defenses. However, the section could benefit from a more detailed analysis of these incidents to extract lessons learned and best practices for prevention.

The section presents a balanced view of personalized learning through AI, highlighting benefits such as customized content, improved engagement, and data-driven insights (Daniel, 2015; Küçük-Demir, 2023; Pane et al., 2015; Walkington, 2013). It also cautions against risks like privacy intrusions, algorithmic bias, and reduced exposure to diverse ideas (Noble, 2018; Regan & Jesse, 2019; Selwyn, 2019; Yanarateş & Yılmaz, 2022). This nuanced perspective aligns with scholarly debates on the ethical implications of AI in education (Williamson & Eynon, 2020; Yılmaz, 2024).

By advocating for transparency, consent and control, purpose limitation, and accountability, the section aligns with fundamental ethical principles in data usage (Floridi, 2016; Mittelstadt et al., 2016; Solove, 2013; Yılmaz, 2023). This framework provides practical guidelines for educators and developers to use data responsibly, emphasizing the importance of ethical considerations in technological advancements.

The strategies suggested for minimizing data collection—data minimization, anonymization, pseudonymization, and local processing—are effective means to protect privacy while maintaining AI functionality (Cavoukian, 2011; El Emam & Arbuckle, 2013; McMahan & Ramage, 2017). Additionally, promoting transparency through explainable AI, user education, and feedback mechanisms fosters trust and empowers users (Abdul et al., 2018; Ananny & Crawford, 2018; Gunning, 2017).

The emphasis on joint efforts in child data protection is a significant strength of the section. By encouraging sharing knowledge, coordinated policies, and support networks, it acknowledges the collective responsibility of parents and educators (Livingstone & Haddon, 2009; Powers & Green, 2018; Yılmaz, 2021b; Zilka, 2017). This collaborative approach is essential in creating a consistent and secure environment for children.

Involving parents in policy development increases relevance, enhances compliance, and fosters trust (Epstein et al., 2018; Shapiro & Stefkovich, 2016). This participatory process ensures that policies reflect community values and concerns, leading to more effective implementation and adherence.

The recommendation for regular security audits helps identify gaps, update practices, and demonstrate commitment to security (Ashford, 2017; Safa et al., 2016; Sevgi & Yılmaz, 2023). Training educators result in practical skills, updates knowledge, and promotes a security culture (Alshammari & Singh, 2018; Johnson, 2012). These measures are vital for maintaining robust security protocols and fostering an environment of continuous improvement.

The suggestion to organize community forums enhances awareness, encourages dialogue, and develops collaborative solutions (Feenberg & Bakardjieva, 2004; Hassani et al., 2018). Such forums can bridge gaps between stakeholders, promote shared understanding, and contribute to the responsible use of AI.

Overall, the section provides a thorough and well-structured examination of privacy and security concerns in AI applications for early childhood education. It effectively integrates legal frameworks, ethical principles, technical measures, and collaborative strategies. The use of relevant and current academic references strengthens the arguments and situates the discussion within the broader scholarly context.

To further enhance the section, it could include more detailed case studies to illustrate the practical application of the proposed measures. Additionally, exploring challenges in implementing these strategies, such as resource constraints or varying levels of digital literacy among parents and educators, could provide a more comprehensive view.

7. References

Abdul, A., Vermeulen, J., Wang, D., Lim, B. Y., & Kankanhalli, M. (2018). Trends and Trajectories for Explainable, Accountable and Intelligible Systems. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-18.

Aksoy, N. C., & Küçük Demir, B. (2019). Matematik Öğretiminde Dijital Oyun Tasarlamanın Öğretmen Adaylarının Yaratıcılıklarına Etkisi. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 39*(1), 147-169.

Almohri, H. M., Childers, B. R., & Das, R. (2016). Secure Execution of Applications on Untrusted Platforms. *ACM Computing Surveys*, 48(2), 1-29.

Alqahtani, M., Alqahtani, A., & Haron, H. (2019). Cybersecurity Awareness Training: The First Line of Defense. *Journal of Information Security and Cybercrimes Research*, 2(1), 3-14.

Alshammari, R., & Singh, D. (2018). A Framework to Integrate Cybersecurity into Education. *Journal of Theoretical and Applied Information Technology*, 96(15), 4910-4922.

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, 20(3), 973-989.

Ashford, W. (2017). Cyber security skills gap is a threat to UK business. *Computer Weekly*.

Aydoğdu, B., Duban, N., & Özdinç, F. (2019). Fen öğretiminde gerçek ve sanal laboratuvarların kullanımı. A. Günay Balım (Edt.). *Fen öğretiminde yenilikçi yaklaşımlar* içinde (ss.307-321). Ankara: Anı Yayıncılık.

Ayyıldız, P., & Yılmaz, A. (2021). Putting things in perspective: The COVID-19 pandemic period, distance education and beyond. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi,9*(6), 1631-1650. https://doi.org/10.18506/anemon.946037

Ayyıldız, P., Yılmaz, A., & Baltacı, H.S. (2021). Exploring digital literacy levels and technology integration competence of Turkish academics. *International Journal of Educational Methodology*, *7*(1), 15-31. https://doi.org/10.12973/ijem.7.1.15

Baker, T., & Smith, L. (2019). *Educ-AI-tion Rebooted? Exploring the future of artificial intelligence in schools and colleges*. Nesta.

Barth, S., & de Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, 34(7), 1038-1058.

BBC News. (2019). Schools hit by cyber-attack. *BBC News*.

Bellman, R.E. (1978). *An introduction to artificial intelligence: Can computers think?* Boyd & Fraser Publishing Company.

Bers, M. U. (2018). Coding as a Playground: Programming and Computational Thinking in the Early Childhood Classroom. *Routledge*.

Bishop, M. (2018). Computer Security: Art and Science. *Addison-Wesley Professional*.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, 1-15.

Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles. *Information and Privacy Commissioner of Ontario*.

Chaudron, S., Di Gioia, R., & Gemo, M. (2018). *Young Children (0-8) and Digital Technology: A Qualitative Study across Europe*. European Commission.

Chen, W., & Li, Q. (2010). Research on AI and multicultural education. *International Conference on E-Product E-Service and E-Entertainment*.

Cimpanu, C. (2017). Edmodo hacked, millions of user accounts up for sale on dark web. *Bleeping Computer*.

Daniel, B. (2015). Big Data and analytics in higher education: Opportunities and challenges. *British Journal of Educational Technology*, 46(5), 904-920.

Donohue, C., & Schomburg, R. (2017). Technology and Interactive Media in Early Childhood Programs: What We've Learned from Five Years of Research, Policy, and Practice. *Young Children*, 72(4), 72-78.

El Emam, K., & Arbuckle, L. (2013). Anonymizing Health Data: Case Studies and Methods to Get You Started. *O'Reilly Media, Inc*.

Epstein, J. L., Sanders, M. G., Sheldon, S. B., Simon, B. S., Salinas, K. C., Jansorn, N. R., & Van Voorhis, F. L. (2018). *School, family, and community partnerships: Your handbook for action*. Corwin Press.

European Commission. (2018). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union.

Federal Trade Commission. (2013). *Children's Online Privacy Protection Rule*. FTC.

Feenberg, A., & Bakardjieva, M. (2004). Virtual community: No "killer implication". *New Media & Society*, 6(1), 37-43.

Ferreira, A., Antunes, L., & Chadwick, D. W. (2014). Security and privacy issues in electronic health records. *Handbook of Research on Advanced ICT Integration for Governance and Policy Modeling*, 330-352.

Floridi, L. (2016). The ethics of information. *Oxford University Press*.

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*, *1*(1), 1-3.

Floridi, L., Cowls, J., Dennis, M., Epstein, M., Stahl, B. C., Taddeo, M., King, T. C., Koenig, A., Lanza, B., Viganò, D. E., Cappelen, C., Cheli, F., Smart, B., Andersson, J., & Savulescu, J. (2018). AI4People—An Ethical

Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines, 28*(4), 689-707.

Gašević, D., Dawson, S., & Siemens, G. (2015). *Learning analytics and learning theory: A critical perspective*. Learning Analytics Review, 6.

Gunning, D. (2017). Explainable Artificial Intelligence (XAI). *Defense Advanced Research Projects Agency (DARPA)*.

Hassani, H., Huang, X., & Silva, E. (2018). Digitalisation and big data mining in banking. *Big Data and Cognitive Computing*, 2(3), 18.

Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. *Center for Curriculum Redesign*.

Holmes, W., Porayska-Pomsta, K., Holstein, K. *et al.* Ethics of AI in Education: Towards a Community-Wide Framework. *Int J Artif Intell Educ,* 32, 504–526 (2022). https://doi.org/10.1007/s40593-021-00239-1

Huang, C., & Zhu, Y. (2019). Ransomware: A security disaster in the education industry. *Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1-8.

Huang, L., Siegel, C., & Robertson, E. (2020). Cybersecurity education: The role of pre-college programs. IEEE Security & Privacy, 18(2), 85-89.

ICO. (2018). Guide to the General Data Protection Regulation (GDPR). *Information Commissioner's Office*.

IEEE. (2019). *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*. IEEE.

Jansen, J., & van Schaik, P. (2019). Persuading vulnerable online users to strengthen password security. *Computers in Human Behavior*, 90, 24-35.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389-399.

Johnson, D. G. (2012). Computer Ethics. *Prentice Hall*.

Johnson, M., Smith, K., & Davis, R. (2016). Can they hack it? Cybersecurity education in the high school classroom. *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, 68-73.

Kallberg, J. (2016). Strategic cyberattack aggregation: A study in destructive efficiency. *Computers & Security*, 58, 109-118.

Kidron, B., & Rudkin, A. (2020). *Young children and digital technology: A rights-based approach*. 5Rights Foundation.

Küçük-Demir, B. (2023). Öğretmen adaylarının şekilsel yaratıcılıklarının incelenmesi. *Uluslararası Eğitim Bilim ve Teknoloji Dergisi, 9*(3), 112-121.

Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., & Verdoodt, V. (2018). Children's rights and digital technologies. *Handbook of Children and Youth Studies*, 1-14.

Livingstone, S., & Blum-Ross, A. (2020). *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives*. Oxford University Press.

Livingstone, S., & Byrne, J. (2018). Parenting in the digital age: The challenges of parental responsibility in comparative perspective. *Contemporary Social Science*, 13(2), 123-136.

Livingstone, S., & Haddon, L. (2009). EU Kids Online: Final Report. *London School of Economics & Political Science*.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). Children's data and privacy online: Growing up in a digital age. *London School of Economics & Political Science*.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. *CO Short Report Series on Key Topics*, 2.

Long, D., & Magerko, B. (2020). What is AI Literacy? Competencies and Design Considerations. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-16.

McMahan, B., & Ramage, D. (2017). Federated learning: Collaborative machine learning without centralized training data. *Google Research Blog*.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys*, *54*(6), 1-35.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21.

Nemorin, S. (2017). The frustrations of digital artefacts in the classroom. *Learning, Media and Technology*, 42(4), 400-413.

NIST. (2018). Computer Security Incident Handling Guide. *National Institute of Standards and Technology*.

Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. *NYU Press*.

Öztürk, B. (2023). Relation of 21st-Century Skills with Science Education: Prospective Elementary Teachers' Evaluation. *Educational Academic Research,* (*50*), 126-139.

Öztürk, B., & Demiroğlu Çiçek, S. (2024). The Effects of Writing to Learn Activities on the 10th Grade on Teaching of Ecosystem Ecology. *Kastamonu Education Journal, 32*(4), 652-667.

Pane, J. F., Steiner, E. D., Baird, M. D., & Hamilton, L. S. (2015). Continued Progress: Promising Evidence on Personalized Learning. *RAND Corporation*.

Passey, D., Bottino, R. M., Carrillo, J., & Tatnall, A. (2018). Teacher Professional Development in the Use of Technology. *Education and Information*

Technologies, *23*(1), 317-343.Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. *IBM Security*.

Ponemon Institute. (2019). *2019 Cost of a Data Breach Report*. IBM Security.

Powers, J., & Green, M. F. (2018). Principals' perspectives on social media in schools. *NASSP Bulletin*, 102(4), 279-292.

Regan, P. M., & Jesse, J. (2019). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology*, 21(3), 167-179.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Santos, O. C., Boticario, J. G., Salmerón-Majadas, S., Pavlopoulou, A., Rodríguez-Ascaso, A., Brooke, J., Montandon, L., Grawemeyer, B., Peters, D., & Brooks, T. (2016). Affective computing in education: A review of current progress and future challenges. *IEEE Transactions on Learning Technologies*, *10*(4), 1-13.

Schneider, B., Ehrhart, M. G., & Macey, W. H. (2015). Organizational climate and culture. *Annual Review of Psychology*, 64, 361-388.

Selwyn, N. (2019). What's the problem with learning analytics? *Journal of Learning Analytics*, 6(3), 11-19.

Selwyn, N., & Gašević, D. (2020). The datafication of education: A critical approach to emerging analytics technologies and practices. *Learning, Media and Technology*, *45*(2), 1-7.

Sevgi, M., Ayyıldız, P., & Yılmaz, A. (2023). Eğitim bilimleri alanında yapay zekâ uygulamaları ve uygulamaların alana yansımaları. Ö. Baltacı (Ed.). *Eğitim Bilimleri Araştırmaları-IV içinde* (ss.1-18). Gaziantep: Özgür Yayınları.

Sevgi, M., & Yılmaz, A. (2023). Yükseköğretimde dijital dönüşüm ve metaverse. Y. Doğan ve N. Şen Ersoy (Edts.). *Eğitimde Metaverse Kuram ve Uygulamalar içinde* (ss.71-86). İstanbul: Efe Akademi Yayınları.

Shapiro, J. P., & Stefkovich, J. A. (2016). Ethical Leadership and Decision Making in Education. *Routledge*.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126, 1880-1903.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Children's data and privacy online: Growing up in a digital age. *New Media & Society*, 22(12), 2164-2185.

Taylor, E., & Rooney, T. (2017). Surveillance futures: Social and ethical implications of new technologies for children and young people. *Routledge*.

Tisdale, K. (2015). Cybersecurity education and awareness in the classroom: A guide for teachers. *Journal of Digital Learning in Teacher Education*, 31(4), 159-164.

UNESCO. (2019). *Beijing Consensus on Artificial Intelligence and Education*. UNESCO.

United Nations. (1989). *Convention on the Rights of the Child*. UN General Assembly.

van der Hof, S. (2016). I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal*, *34*(2), 409-445.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6), eaan6080.

Walkington, C. (2013). Using adaptive learning technologies to personalize instruction to student interests: The impact of relevant contexts on performance and learning outcomes. *Journal of Educational Psychology*, 105(4), 932-945.

Williamson, B., & Eynon, R. (2020). Historical Threads, Missing Links, and Future Directions in AI in Education. *Learning, Media and Technology*, 45(3), 223-235.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. *National Institute of Standards and Technology*.

Yanarateş, E., & Yılmaz, A. (2022). Fen öğretiminde 21.yüzyul becerilerinin önemi. S. Karabatak (Ed.). *Eğitim ve Bilim 2022-III içinde* (ss.75-90). Efe Akademi Yayınları.

Yılmaz, A. (2021a). The effect of technology integration in education on prospective teachers' critical and creative thinking, multidimensional 21st century skills and academic achievements. *Participatory Educational Research, 8*(2), 163-199. https://doi.org/10.17275/per.21.35.8.2

Yılmaz, A. (2021b). Fen bilimleri eğitimi kapsamında uzaktan eğitimde kalite standartları ve paydaş görüşleri. *Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi Dergisi, 42*, 26-50. https://doi.org/10.33418/ataunikkefd.850063

Yılmaz, A. (2023). Fen bilimleri eğitiminde dijital uygulamalar, yapay zekâ ve akıllı yazılımlar: Tehditler ve fırsatlar. A. Akpınar (Ed.). *Matematik ve Fen Bilimleri Üzerine Araştırmalar-II* içinde (ss.1-20). Gaziantep: Özgür Yayınları.

Yılmaz, A. (2024). Enhancing the Professional Skills Development Project (MESGEP): An Attempt to Facilitate Ecological Awareness. *Participatory Educational Research, 11*(1), 16-31. https://doi.org/10.17275/per.24.2.11.1

Yılmaz, A., Gülgün, C., Çetinkaya, M., & Doğanay, K. (2018). Initiatives and new trends towards STEM education in Turkey. *Journal of Education and Training Studies, 6*(11a), 1-10.

Yılmaz, A., & Salman, M. (2022). Investigation of the Relationship Between Pre-service Teachers' Critical Thinking Dispositions and Attitudes Towards Socioscientific Issues. *E-Uluslararası Eğitim Araştırmaları Dergisi, 13*(1), 203-219. https://doi.org/10.19160/e-ijer.1054393

Yılmaz, A., Şahin-Atılgan, K., & Güzel-Sekecek, G. (2024). Sürdürülebilir kalkınma ve eğitim. M. Korucuk (Ed.). *Eğitimin Temellerine Bakış: Program Geliştirme-Yeni Yaklaşımlar içinde* (ss.225-236). İstanbul: Efe Akademi Yayıncılık.

Yılmaz, A., Uysal, G., & Nacar, M. (2024). Düşünme becerilerine (yaratıcı, yansıtıcı, eleştirel ve problem çözme) bakış. M. Korucuk (Ed.). *Eğitimin Temellerine Bakış: Program Geliştirme-Yeni Yaklaşımlar içinde* (ss.165-180). İstanbul: Efe Akademi Yayıncılık.

Zhao, Y., Xu, X., & Wang, M. (2019). Rethinking data privacy laws in the era of big data: A comparative legal analysis. *Laws*, 8(3), 17.

Zhu, Z. T., & Xie, H. H. (2019). Application of Artificial Intelligence in Early Childhood Education. *Journal of Physics: Conference Series*, 1237.

Zilka, G. C. (2017). Awareness of eSafety and potential online dangers among children and teenagers. *Journal of Information Technology Education: Research*, 16, 319-338.