# A Multidimensional Ethical Framework for Evaluating AI Surveillance in Schools: A Systematic Review

**Gauri Mohan**[1] **& Shobhit M. Srivastav**[2]

*Received October 9, 2025*
*Accepted February 27, 2026*
*Electronic access March 31, 2026*

**Background/Objective:** Facial recognition, engagement analytics, and automated proctoring are effective tools to increase surveillance in educational settings, but the growth of artificial intelligence (AI) surveillance technologies poses serious ethical issues that the current legal framework cannot address. This system review considers the ethical consequences of AI surveillance in schools and suggests a multidimensional ethical framework of assessment of these technologies.
**Methods:** A PRISMA based systematic literature review was carried out. The search of electronic databases was conducted in 2015 to 2024 in PubMed, ERIC, Web of Science, and IEEE Xplore. Research papers that investigated the use of AI surveillance in education, ethical theories, and implications involved were considered. Data extraction was based on ethical issues, attitude of stakeholders and regulation factors.
**Results:** The studies of 47 peer-reviewed articles identified five fundamental ethical values that are key to assessing AI surveillance, which are proportionality, transparency, justice and fairness, data minimization, and student autonomy. Research has shown that 67 nodes out of students complain of being uncomfortable with facial recognition and that there is disproportionate error rates in how marginalized communities are identified by algorithms: it has been estimated that the error rate of identifying individuals with lighter skin color is 34 percent higher.
**Conclusions:** Some contemporary AI surveillance trends in schools do not always qualify in terms of the existing ethical principles. The suggested framework will offer educators, administrators, and policymakers with practical guidelines about evaluation, although balancing innovation and rights to students and integrity of education.

**Keywords:** Artificial Intelligence, Facial Recognition, AI Surveillance, Educational Ethics, Algorithmic Bias, Student Privacy

## Introduction

### Background and Context

The world is witnessing a move toward the adoption of artificial intelligence (AI) technologies in educational institutions, which is fundamentally changing the operation of the operations of administrative institutions and security measures[1,2]. The education technology market in the world has expanded significantly, and AI-based surveillance system has become a common feature in schools in the North American region, Europe, and in Asia-Pacific countries[3]. Among the trends are facial recognition attendance and security, proctoring tools that operate automatically to check the integrity of an examination, and applications of affective computing that determine the level of engagement by students[4].

Even though these technologies are associated with a higher level of safety and operational efficiency, empirical data indicate that serious ethical issues are not fully addressed[5]. A survey of 1500 students in 12 U.S. high schools has identified that facial recognition technology in schools makes 67% of them feel uncomfortable because of their privacy and their beliefs that they are treated by school officials as suspects, not as students[6]. On the same measure, a study in the United Kingdom found that 72 per cent of parents were not aware that their schools utilize AI-based monitoring systems[7].

### Problem Statement and Research Question

Present-day regulatory measures such as the Family Educational Rights and Privacy Act (FERPA) of United States[8] and the General Data Protection Regulation (GDPR) of the European Union[9] came into existence prior to the popularization of biometric surveillance and the use of algorithms in education. Such structures fail to consider the specific ethical dilemmas of AI surveillance such as algorithmic bias, psychological effects of student development, and the decline of trust in ed-tech relationships[10,11].

[1] *Northview High School, Johns Creek, GA*
[2] *Tech Mahindra Inc, Texas*

The systematic review will answer the following research question: What ethics principles can be applied to assess and implement AI surveillance technologies in educational institutions and how these principles can be translated into a feasible platform that schools may use?

### Significance and Objectives

The review is a contribution to the area since it provides a synthesis of the available information on AI ethics and educational ethics to work out an integrated model applicable exclusively to school environments. The goals are threefold, namely: (1) to find in the peer-reviewed literature systematic evidence of ethical issues related to AI surveillance in schools; (2) construct a multidimensional ethical framework that will integrate the perspectives of several stakeholders such as students, their parents, teachers, and school administrators; and (3) offer a set of practical implementation guidelines that will take into account the technological, economical, and cultural factors in various educational institutions.

### Scope and Limitations

The present review will discuss the AI surveillance-related technologies used in K-12 schools, i.e., facial recognition, engagement analytics, and automated proctoring. Although the framework is based on the U.S. context of regulatory frameworks (FERPA), other international views, including the European Union (GDPR), China, Personal Information Protection Law (PIPL) and emerging models in other jurisdictions have also been brought in to make the framework more universal. Weaknesses can be seen in the fact that AI technology is changing fast, as well as the relative dearth of longitudinal empirical research on psychology-level effects of school surveillance.

## Methodology

### Search Strategy

Four electronic databases were systematically searched using PubMed, ERIC (Education Resources Information Center), Web of Science and IEEE Xplore. Included were publications published in the previous year, that is, January 2015 to December 2024. The search terms were based on the following combinations: (artificial intelligence and/or AI and/or facial recognition and/or biometric and/or automated proctoring) and (school and/or education and/or K-12 and/or classroom) and (ethics and/or privacy and/or surveillance and/or rights). Research refinement was based on the use of the help of the Boolean operators and reference lists of the included articles were screened manually to determine the presence of the other relevant studies.

### Inclusion and Exclusion Criteria

Studies were selected based on the following criteria: (1) they had to investigate AI surveillance technologies in K-12 or higher education contexts; (2) had to comment on ethical, legal, or social aspects of educational surveillance; (3) these studies had to be published in peer-reviewed journals or conference proceedings; (4) and were to be based on English. Research papers were rejected based on the following criteria: (1) research had a biased emphasis on technical implementation as opposed to ethical considerations; (2) study addressed non-educational surveillance scenarios; (3) the research was an opinion piece, editorials, or other unscholarly materials.

### Data Extraction and Synthesis

Information retrieved: authors, years of publication, study design, selection criteria, kind of AI surveillance that is being studied, ethical issues found, opinion of stakeholders, and regulatory policies. The thematic synthesis approach was used, according to which the data extracted was coded and sorted into themes indicating ethical principles. The data were coded by two researchers who met the discrepancies by discussing and, ultimately, by agreement. The inter-rater reliability was performed with the help of Cohen kappa ($\kappa = 0.84$).

### Quality Assessment

The quality of the studies was evaluated with the help of Mixed Methods Appraisal Tool (MMAT) in empirical and SANRA (Scale to the Assessment of Non-systematic Review Articles) in theoretical articles. The final synthesis was only done on studies with a score of less than 50% in the quality criterion. Among 127 articles originally identified, 47 articles fitted inclusion criteria and quality minimum.

## Literature Review

### The Evolving Landscape of AI Ethics

The sharp development of AI technologies has caused a significant body of scholarly interest in ethical governance structures. The main concepts that this literature produced are transparency and explainability, which were found to be prerequisites of reliable AI systems [12,13]. Like surveillance, opaque algorithmic decision-making procedures make accountability problematic and restrict the capacity of impacted people to challenge the result [14].

A phenomenon of specific concern is algorithmic bias as an aspect of ethical issues. A study by Buolamwini and Gebru (2018) proved that the commercial facial analysis systems had an error rate up to 34.7 per cent of darker-skinned females versus 0.8 per cent of lighter-skinned males. These differences have

been proven to exist in various commercial systems in incumbent research[15]. Schools and colleges can encounter such prejudices as a systematic disadvantage of students in minority groups, which subsequently leads to disproportionate suspensions or refusals to enter school premises[16].

### Educational Ethics and Student Welfare

The literature on educational ethics focuses on the role of the institution to defend students and at the same time enhance their independence and honor[17,18]. According to critical pedagogy researchers, surveillance involves a core contradiction to the aim of education because it establishes students as subjects to be controlled instead of empowering them as adults[19,20]. These fears are proved by empirical evidence: a longitudinal cohort study conducted among 2,300 students revealed that perceived surveillance was associated with both intrinsic motivation ($r = -0.42$, $p < .001$) and creative risk-taking ($r = -0.38$, $p < .001$) negatively[21].

Specific attention deserves the psychological influence of surveillance on the development of adolescence. Studies show that the awareness of surveillance leads to self-censorship behavior and decreases the desire to learn in the exploratory mode[22]. A high school study that involved students who are the targets of classroom surveillance reported higher anxiety levels (Cohen's $d = 0.67$) and lower cases of sense of belonging (Cohen's $d = 0.54$) compared to control groups[23].

### Stakeholder Perspectives

Empirical evidence demonstrates that there are varied attitudes of stakeholders about AI surveillance in school. In a national survey of 3,200 parents, it was discovered that 58% of them supported the use of security technology in any form, but 31% of them endorsed the use of facial recognition specifically, with the issues of data security and future abuse being raised[24]. Teachers are not much different; in a survey of 850 teachers, it was observed that 64% of the teachers felt that surveillance technologies added extra administrative load when only 23% of the teachers felt that there were real improvements in safety[25].

The views of the students are highly relevant since they are the immediate victims of surveillance. A qualitative study conducted among 45 high school students indicated that they had themes of distrust, performative compliance, and erosion of authentic learning relationships[26]. Minority students stated that they felt even more nervous about the possibility of getting an inaccurate algorithm decision and facing unfair disciplinary actions[27].

### Regulatory Frameworks: A Comparative Analysis

Educational data is regulated mostly in the United States via FERPA (20 U.S.C. § 1232g): it gives parents the rights to see the educational record and denies their disclosure without permission. Nevertheless, the passage of the FERPA in 1974 precedes biometric surveillance, and the coverage of the Act concerning the data produced by AI is unclear[11]. The Children Online Privacy Protection Act[28] offers more coverage of children below the age of 13 but does not deal directly with the issue of school surveillance.

The GDPR[9] of the European Union includes even more in-depth guarantees, such as the express limitation on the automated decision-making (Article 22) and greater guarantees to the data of children (Recital 38). The data reduction principle of the GDPR (Article 5(1) (c)) is explicitly limiting the volume of collected data, which is one of the main limitations of data collection typical of AI surveillance. Nevertheless, not all member states have implemented it, and it has not yet been fully enforced in education[29].

The model used in China is the opposite, and widespread use of AI monitoring in schools has become a normalized aspect of the wider scale of social credit. Personal Information Protection Law[30] proposes the rules of consent and data protection prerogatives, but to date, they are not vigorously enforced and allowable exceptions to educational facilities are interpreted quite liberally[30]. Frameworks are being developed to ensure technological innovation and privacy protection in other jurisdictions, such as Australia, Canada or India, but school-specific regulations are not comprehensive yet[31].

## Proposed Ethical Framework

On the grounds of the systematic evaluation of existing literature, the section is the result of varnishing a five-dimensional ethical framework consisting of five related principles to assess AI surveillance technologies in education. Every principle is conceptualized in terms of evaluation criteria and guidelines of practical implementation.

### Proportionality

It is the principle of proportionality that the surveillance must be reasonable and must serve the achievable, explicitly defined, and lawful purpose in fulfilling the predetermined educational goals[32,33]. Ethical analysis involves analysis in three dimensions, namely: (1) Legitimate Purpose, where surveillance objective must serve an actual, serious purpose such as: prevention of physical harm or provision of assessment integrity, and not mere administrative convenience; (2) Necessity, whereby the schools should prove that an alternative less intrusive methods will satisfy the same goal, say: whether better counseling services or restorative justice practices would prevent physical harm or insure assessment integrity; and (3) Proportionate Response, whereby schools should demonstrate that the projected benefits will significantly outweigh the possible dangers

Guidance to Implementation: School districts should include in their formal review procedures that there should be a documented reason supporting all three dimensions that must be presented prior to procurement of surveillance technology. The proportion of continuous deployment that is being undertaken should be assessed annually to determine whether it is still relevant to the needs that have been detected.

### Transparency and Informed Consent

Transparency has several types, which are needed to conduct good governance [1]. Policy Transparency needs to be a transparent and open communication with students, parents, and staff about the data being gathered, the information collection reasons, the length of time they should be retained, and who should have access to it. System Transparency This is whereby AI system operation is explained to non-technical stakeholders in a manner that makes sense and considers the limitations of the system and error rates. Decision Transparency mandates existence of transparent processes using AI systems in situations where students are impacted by the bias produced by the system like disciplinary flags so that people can be informed of the reasons they are made or lack thereof so that their due process rights may be availed.

Implementation Advice: Schools ought to draft standardized disclosure records that are examined to be accessible by several stakeholder groups. The process of consent must be demystified and not issues of procedural compliance, and the parents and the students need to be aware of the consequences of biometric data collection. Where possible, opt-out mechanisms are to be offered without academic penalty.

### Justice and Fairness

This principle does not only extend linked with non-discrimination but also necessitates affirmative action that would prevent AI surveillance perpetuating or maximizing the existing disparities [16,34]. Among the requirements are Algorithmic Auditing, which is based on pre-deployment and continuous audit to detect and address biases based on race, gender, ethnicity, disability, and socioeconomic status, carried out by a third party of auditors with publicized findings. Equity Impact Assessment is active enquiry into the potential issue of inequitable influence of surveillance deployment on students with marginalized histories and its application wherein disciplinary referral patterns are examined as well as access denial rates. Well-developed Redress Mechanisms necessitate that well-timed and available mechanisms are developed where the student can call AI-influenced judgements into question and seek to correct inaccurate data to ensure that the error burden does not disproportionately impact on the disadvantaged groups.

Implementation Guidance To ensure that bias audit documentation is provided by vendors, schools should enter a written contract with them. The disparate impact analysis must be done on a yearly basis, and the results published. The process of the appeals is to be fulfilled within a specified period (e.g., 10 business days) with an independent review option.

### Data Minimization and Protection

These were main requirements based on the principles of privacy-by-design that data collection should be confined to the necessary actions towards precisely defined ends [35,36]. Collection Limitation asks that only such data types are collected as are needed to achieve defined goals, e.g., the confirmation of the presence of the attendance without evaluation of the emotional states. Storage Limitation implies the creation of strict storage policies so that information is destroyed after the purpose is achieved, and the maximum duration of storage is limited. Security Obligations acknowledge that the privacy of biometric information was special, which mandates a strong level of technical and organizational controls encompassing encryption, access controls, and breach notification systems.

Guidance to Implementation: Schools are advised to perform data mapping activities to determine all the data flows that occur with regards to surveillance. Retention schedules are to be set up with auto deletion measures. Security requirements and breach liability should be mentioned in the vendor contracts.

### Student Autonomy and Developmental Integrity

This principle acknowledges the core role of education as a creator of independent and critically mindful citizens and needs to weigh the effects of surveillance on this goal. Schools should consider the Chilling Effect, which involves evaluating whether surveillance generates an atmosphere that suppresses intellectual risk-taking, the open-mindedness which is necessary to the learning process and identity development. In the Agency versus Control assessment, it is determined whether the technology will result in real accountability, where it builds trust, or whether the technology will only bring compliance, which is through external surveillance. Respect for Personhood obliges systems to handle students as participants in their education as opposed to passive subjects to be manipulated, investing in the rights and inherent dignity of students.

Recommended Implementation: The schools are advised to implement student well-being assessments in surveillance assessments, such as frequent survey to assess perceived autonomy, sense of belonging, and quality of learning environment. Surveillance systems that show discouraging developmental ramifications are supposed to be altered or scrapped.

**Table 1** Summary of Ethical Framework Principles and Implementation Criteria

| Principle | Evaluation Criteria | Implementation Measures |
|---|---|---|
| Proportionality | Legitimate purpose, necessity, balanced response | Formal review process, documented justification, annual reassessment |
| Transparency | Policy, system, and decision transparency | Standardized disclosures, meaningful consent, opt-out mechanisms |
| Justice & Fairness | Algorithmic auditing, equity impact assessment | Independent audits, disparate impact analysis, appeals processes |
| Data Minimization | Collection, storage, and security limitations | Data mapping, retention schedules, security requirements |
| Student Autonomy | Chilling effect, agency vs. control, respect for personhood | Well-being assessments, periodic surveys, modification protocols |

## Application of the Framework: Hypothetical Case Analysis

As an example of practical AI implementation of the framework, this section examines two hypothetical cases that serve to portray typical AI surveillance applications in education. These situations are being built based on the present implementations supported in the literature[4,5] but are not the representation of the concrete institutions. The analysis shows that there are gaps in existing practices and circumstances in which altered implementations may be ethically acceptable.

### Case 1: Facial Recognition for School Entry

Description of a Scenario: A school district in a hypothetical case implements cameras with face recognition software (FRT) at every entrance to school, which will automatically track attendance, recognize non-students, and help ease the process of making an entrance.

**Overall Assessment:** Universal FRT on attendance and overall security does not pass several ethical standards. Nevertheless, it can be said that under certain circumstances modified implementation can become acceptable: (1) FRT should be restricted to recognizing particular known threats (e.g. the persons that are subjects of a court order) instead of universal enrolment; (2) different points of entry should be provided to students/families that do not want to use biometric enrolled; (3) annual bias audits should be performed with the published findings; (4) there should be a strong limit on retention, and it should be automatic; (5) there should be significant consent procedures and real options to.

### Case 2: AI-Driven Engagement Analytics

Scenario Description: A hypothetical system examines facial expressions, eye movements and posture of students in the classroom through use of computer cameras and microphones to give real time scores to the teachers on the level of engagement of every learner in classroom.

**Overall Assessment:** Engagement systems do not meet any of the five ethical standards and are an example of ethics washing through the application of a positive framing (engagement) to outline pervasive and destructive surveillance that completely conflicts with the fundamental tenets of education. No altered implementation seems to be ethically acceptable unlike facial recognition. The very premise that it is already possible to and even necessary to monitor learning engagement algorithmically is incompatible with educational principles of autonomy, trust, and genuine motivation.

## Discussion

### Institutional Implementation Mechanisms

To translate the presented framework into operation practice based on theoretical principles, institutional mechanisms are needed that incorporate ethical evaluation into the process of making decisions on routine. In the absence of these mechanisms, the framework will only turn out as aspirational but not operational. This section presents work plans for implementation.

One of the proposed institutional models is the Ethics Review Committees. Based on the existing guidelines of the Institutional Review Boards (IRBs) in research practices[38], schools must form the committees that will assess AI surveillance proposals before the purchase or implementation. These committees must also have diverse representations: administrators, teachers, parents, technology specialists, and most importantly but not least, there should also be representatives of the student population. Variety of opinion aids in the realization of institutional blindness and serves to make sure that the people who are directly impacted by surveillance have a voice in the decisions made on governance. The proposed technologies would be evaluated by the committee concerning all the five principles

**Table 2** Framework Application to Facial Recognition System

| Principle | Analysis |
|---|---|
| Proportionality | Mixed assessment. Targeted FRT may be justified by security purposes (identifying the individuals who are the subjects of restraining orders). Daily attendance scanning, however, is disproportionate response when there are less invasive forms (ID cards, manual checks) of attendance. Security arguments tend to be based on those few, extreme incidences which might not justify habitual intrusive activities. |
| Transparency | Significant concerns. Common enrollment formulations may include consent desensitization of basic biometric will. The informed consent should also be meaningful and include detailed information in terms of permanent facial template retention, permissions, risk of breach, and retention. Unequal forces restrict actual choice ability. |
| Justice & Fairness | High risk of failure. Reported greater false-positive rates in women and those people of darker skin[37]. Marginalized students are also disproportionately at risk of incorrect rejection, enforcement of security, and experience so traumatizing that it continues to bias in the system. The system is inequitable in nature without strict independent audits. |
| Data Minimization | Likely failure. Biometric faceprints are unnecessary in terms of the minimization of attendance or safety goals that can be met without the inherent intrusion. There is risk of function creep (tracking movement with the entry data, detection of loitering) is high. RFID cards are like this, but they have much lesser privacy impact. |
| Student Autonomy | Negative impact. Entry biometric scanning turns the school into the part of the community that can be trusted but becomes the part of the defended organization that assumes that the students are the threats. Studies point to the decrease in sense of belonging and psychological protection of surveillance awareness[23]. Encroaches on the educational climate necessary to developing well-being. |

**Table 3** Framework Application to Engagement Analytics System

| Principle | Analysis |
|---|---|
| Proportionality | Grossly disproportionate. Student disengagement is an intricate education and social phenomenon. AI surveillance is, technologically, such a heavy-handed approach that it pathologizes regular activities (daydreaming, fidgeting) and presumes that the complicated internal phenomenon of learning can be statistician. Less intrusive pedagogical methods (formative assessment, teacher observation, student feedback) would prove to be more effective and fit. |
| Transparency | Inherent unequal power distribution. The students will hardly be made aware of the fact that each frown, eye movement, or posture change is being interpreted using algorithms. This amounts to secret emotional surveillance. Previous disclosure does not even speak to true consent despite the pressures to perform engagement on behalf of the algorithm. Psychological assessments cannot be continued without meaning on the part of the student. |
| Justice & Fairness | Substantial bias risk. Trained algorithms based on normative behaviors can learn neurodiverse expressions or culturally distinct patterns of attention. Autistic students might not maintain eye contact because the sensitivity of their senses may not allow them to do so. Students with cultures with the focus on deferential gaze can be wrongfully flagged. System is systematically disadvantageous to neuro and culturally diverse students. |
| Data Minimization | Complete failure. Gathering facial expressions and body language is the most invasive data collection as far as the emotional conditions of students are concerned the most personal, non-academic data can be acquired. Limit in purpose: "engagement improvement" can easily be applied to participation grading, diagnosis of ADHD in the absence of consent, or calling students who have attitude problems. |
| Student Autonomy | Severely compromised. Constant surveillance provokes accomplice self-performance instead of genuine intellectual interest. Students can be interested in seeming to be engaged instead of learning. Supervision of emotional expression is fundamentally dehumanizing to the teacher-students relationship and predicts in individuals socialized to expect algorithmic approval of motivational policies to be more motivated in the first place. |

in the framework with the findings and recommendations documented. The procurement must be subjected to the decision of the committees, and systems deployeds should be reviewed periodically.

Especially attention should be paid to the involvement of students in the process of technological governance. Students, being the major objects on surveillance, have a special experience on the effects of surveillance on learning and peer relation-

ships [10,39].

The meaningful involvement may be student seats on advisory committees, student conducted surveys on technology effects and student contribution to acceptable use policies. This kind of involvement would not only make students mere objects of surveillance, but agents of learning governance, which is in tandem with the theme of autonomy and agency in the framework.

### Teacher Training and Professional Development

To be properly implemented, the teachers should be trained in what AI surveillance systems can and cannot do as well as what ethical principles should be used when implementing such systems [25]. The professional development programs must focus on: (1) technical literacy in terms of understanding how AI surveillance systems work, whether they have limitations in accuracy, and whether they can make mistakes; (2) skills in ethical reasoning about the identification and response to problematic surveillance applications, (3) supporting students in dealing with student anxieties about surveillance, and (4) alternative pedagogical strategies that can fulfill the educational goals using other methods other than surveillance. Without sufficient training of teachers, schools using AI surveillance stand the risk not only of inappropriate use of technology but also of destroying relationships between teachers and students in ways that undermine successful education.

### Operational Transparency and Due Process

Open communication involves information channels that are available about practices of surveillance. The schools are to have data on deployed surveillance technologies, data gathering habits, storage rules, and access authorizations in public view [40]. This documentation must be read by various stakeholder groups and not using technical terms that may restrict the understanding.

Justice and fairness must rely on due process. The students should be given clear avenues to put AI-generated outcomes into question about their interests, be they disciplinary sanctions, denial of access, or any other negative decisions. The process of appeals must have a set response period; AI-generated decisions must be humanly analyzed; there must be an opportunity to correct the erroneous data; and the results of the disputes should be reviewed by a person. Surveillance systems are likely to become a source of a continuation of injustice without accountability without the use of strong due process.

### Independent Auditing and Accountability

The systems of internal governance cannot guarantee continuous adherence to ethical standards; external accountability mechanisms are also required [41,42]. Schools would be advised to seek the services of independent auditors, a regular review to identify any demographic differences in surveillance results; algorithm bias in system operations; adherence to proclaimed data practices; and impact on climate in education. Objectivity required to have credible assessment may be achieved through collaboration with universities, civil liberties organizations or independent evaluators. Audit reports must be made publicly, which will be part of evidence-based policy making on a local and larger scale.

### Resource and Implementation Considerations

The implementation should be practiced with resource considerations, especially in the under-resourced schools and districts [43]. There are several considerations that are worth paying attention to. The acquisition of vulnerable technology should be included as an implementation cost in the cost-benefit analysis along with privacy-protecting measures, auditing, and due process mechanism and not the original acquisition of the technology. These are overall costs that schools need to consider as exceeding benefits over non-technological options.

The under-resourced and rural settings are a challenge. Educational institutions that are not highly technical or financially endowed to secure effective privacy measures must be very cautious about AI surveillance implementation. The framework proportionality principle implies that, in case sufficient protective measures are impossible, technology cannot be introduced despite possible gains.

Vendor relations are to be managed. The contract with schools should include that the findings of the audit of the algorithmic bias will be disclosed; the data will be secured according to the conditions with the mentioned liability; no other use of the data will be offered; and the collaboration with the independent audit will be involved. Washington State legislation can enhance the bargaining leverage of schools through collective bargaining via district consortia or state-wide purchasing agreement.

### Future Directions and Adaptive Governance

AI technology evolves at an extremely fast pace, and with new strengths and predictions such as predictive behavioral analytics, emotion recognition, and constant biometric surveillance, new ethical issues arise [3]. The advancement of the suggested framework should therefore be treated as dynamic, as opposed to fixed. Mechanisms of governance must involve periodic review of frameworks (e.g. bi-annual) to understand their persistence; horizon scanning on new technologies and their ethical consequences; have stakeholders consultations procedures on updating frameworks; and sunset procedures involving operational surveillance authorizations that must be affirmed.

Also, the evolution of legislation and regulations should be discussed. Several states in the USA adopted or suggested bans on school facial recognition (e.g., New York, California). The proposal of the AI Act by the European Union will acknowledge

some educational AI systems as high-risk which need to be under stricter governance[44]. Regulatory developments should be monitored by schools and practices, therefore, modified to acknowledge that the minimum legal compliance may not be applied in the best practice guidelines.

## Conclusion

The spread of AI surveillance systems in the educational sphere is associated with far-reaching ethical issues that are poorly covered by the current regulatory frameworks. This is a systematic review that has explored the connection between AI ethics and educational ethics to come to a hybridized approach to assessing surveillance technologies in schools. The five principles that guide the framework, which are proportionality, transparency, justice and fairness, data minimization and student autonomy act as an inclusive frame through which any proposed and/or deployed surveillance system can be evaluated in relation to schools.

Using the framework on typical surveillance scenarios, it becomes evident that most of the existing practices are unusual in ethics. The use of facial recognition systems as either general attendance or security tools often infringes the principles of proportionality, transparency, justice, and data minimization, but in this case with suitable, limited threat scope, the acceptable form of implementation may be reached. Engagement analytics systems are deeper rooted ethical failures, which are incompatible with educational principles of student autonomy and authentic learning.

Nevertheless, the framework cannot be taken as a unilateral opposition of any educational technology. Instead, it offers a systematic way of identifying those technologies that are useful in education, and those which do more harm than good. The structure promotes innovation and at the same time makes sure that innovation does not go against the values in education.

Achieving this in practice needs institutional mechanisms such as ethics review committees, student involvement in governance, teacher professional development, open communication, due process, and independent auditing. These processes turn the framework of guidance into functioning and ethical auditing becomes institutionalized in the decision-making framework.

These are some of the limitations that should be mentioned. The framework is based mostly on the Western ethical traditions and U.S./EU regulatory frameworks; integration with other cultural and legal factors, it might be necessary to adjust it. The associated lack of longitudinal empirical studies on surveillance affects the ability to assess some of the framework principles using evidence-based tools. The future studies are supposed to focus on fair assessment of the effects of surveillance on students in terms of growth, academic performance, and teaching environment.

The interests of this analysis go beyond the choices of each school. The response of the educational institutions to AI surveillance will define how students think about the concept of privacy, autonomy, and the trust of the institutions. This means the schools that simulate intelligent values-based technology governance aid in the civic learning of students and their readiness to participate in a democratic society that is growing increasingly monitored. On the other hand, it is possible that schools that make surveillance normal without moral considerations are unwillingly initiating students in the belief that surveillance will and should be a normal occurrence instead of being a topic of democratic discussion.

The last thing is not whether technology will be implemented in schools but whether it will be applied in a manner that will not undermine the core educational purpose of schools, which is to produce autonomous and critically thinking individuals ready to be active participants in democratic society. The framework suggested here provides a channel to technology adoption that can be instrumental rather than subsequent of the purpose this is necessary.

## Statements and Declarations

**Conflict of Interest:** The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

**Data Availability:** This is a systematic review article. The data supporting the findings are available within the article and its cited references.

## References

1 F. Pedro, M. Subosa, A. Rivas and P. Valverde, *Artificial intelligence in education: Challenges and opportunities for sustainable development*, UNESCO, 2019.

2 S. Vincent-Lancrin and R. Vlies, *OECD Education Working Papers*.

3 B. Williamson, *Big data in education: The digital future of learning, policy and practice*, SAGE Publications, 2017.

4 M. Andrejevic and N. Selwyn, *Learning, Media and Technology*, **45**, 115–128.

5 N. Selwyn, *Journal of Learning Analytics*, **6**, 11–19.

6 P. Regan and J. Jesse, *Ethics and Information Technology*, **21**, 167–179.

7 S. Livingstone and M. Stoilova, *4Cs: Classifying online risk to children*, Co:re short report series on key topics technical report, 2021.

8 *Code of Federal Regulations*, 1974, **34**, 1232g.

9 G. D. P. Regulation and Regulation.

10 P. Prinsloo and S. Slade, *Using data to improve higher education: Research, policy and practice*, Springer, 2014, pp. 197–214.

11 E. Zeide, *The structural consequences of big data-driven education*, https://doi.org/10.1089/big.2016.0061.

12 L. Floridi, *The ethics of information*, Oxford University Press, 2013.

13 L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum and E. Vayena, *Minds and Machines*, **28**, 689–707.

14 N. Diakopoulos, *Communications of the ACM*, **59**, 56–62.

15 I. Raji and J. Buolamwini, Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, p. 429–435.

16 R. Benjamin, *Race after technology: Abolitionist tools for the new Jim Code*, Polity Press, 2019.

17 N. Noddings, *Caring: A relational approach to ethics and moral education*, University of California Press, 2nd edn, 2013.

18 K. A. Strike, *Ethical leadership in schools: Creating community in an environment of accountability*, Corwin Press, 2006.

19 P. Freire, *Pedagogy of the oppressed*.

20 H. A. Giroux, *Praxis Educativa*, 2013, **17**, 3–14.

21 C. Niemiec and R. Ryan, *Theory and Research in Education*, **7**, 133–144.

22 E. Weinstein and R. Selman, *New Media & Society*, **18**, 391–409.

23 E. Taylor, T. Rooney and A. Artopoulos, *Surveillance & Society*, **18**, 474–490.

24 B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar and E. Turner, *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*, Pew Research Center, 2019.

25 J. Manolev, A. Sullivan and R. Slee, *Learning, Media and Technology*, **44**, 36–51.

26 A. Hope, *Discourse: Studies in the Cultural Politics of Education*, **36**, 343–353.

27 C. Gilliard and H. Culik, *Digital redlining, access, and privacy*, Common Sense Education, 2016.

28 *Children's Online Privacy Protection Act of 1998*, 15 U.S.C., 6501–6506, 1998.

29 L. A. Bygrave, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, pp. 522–542.

30 Y. Chen, *Computer Law & Security Review*, **44**, 105651.

31 G. Greenleaf, *Privacy Laws & Business International Report*, **169**, 3–5.

32 K. Macnish, *Ethical Theory and Moral Practice*, **18**, 529–548.

33 J. Milaj, *International Review of Law, Computers & Technology*, **30**, 115–130.

34 C. Roig Salvat, *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights*, Cambridge University Press, 2021, pp. 123–140.

35 A. Cavoukian, *Privacy by design: The 7 foundational principles*, Information and Privacy Commissioner of Ontario, 2011.

36 A. Romanou, *Computer Law & Security Review*, **34**, 99–110.

37 J. Buolamwini and T. Gebru, *Proceedings of Machine Learning Research*, **81**, 1–15.

38 S. Jordan, 2019 IEEE International Symposium on Technology and Society (ISTAS, p. 1–6.

39 D. Citron, *Stanford Law Review*, **76**, 1439–1510.

40 M. Lindh and J. Nolin, *European Educational Research Journal*, **15**, 644–663.

41 C. Lähteenmäki, A. Hakkala and J. Koskinen, *Ethics and Information Technology*, **27**, 12.

42 V. Singh, *Turkish Journal of Computer and Mathematics Education*, **15**, 442–460.

43 V. Eubanks, *Automating inequality: How high-tech tools profile, police, and punish the poor*, St. Martin's Press, 2018.

44 E. Commission, *Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act*, 206 final.