The Sankalpa: International Journal of Management Decisions
ISSN: 2454-7425
Volume 12, Issue 1 (January - June 2026)

Legal Protection of the Learner's Personal Data in the Era of Artificial Intelligence

Dr. Sebiane Mohammed
Abu Bekr Belkaid University of Tlemcen; Algeria
mohammed.sebiane@univ-tlemcen.dz
Dr.safraoui fatima
Faculty of Law and Political Science – University of Chlef, Algeria
f.safraoui@univ-chlef.dz

Received :*10/08/2025*   ***Accepted:*** *06/12/2025*   ***Published :****25/03/2026*

Abstract :

This study addresses an important issue concerning the effectiveness of existing legal rules in protecting learners' digital privacy in light of the widespread use of artificial intelligence technologies in the education sector. As educational institutions increasingly adopt adaptive learning platforms and intelligent tutoring systems, the collection of learners' personal and behavioral data has become a technical necessity for operating these systems. The study aims to highlight the main legal challenges posed by these technologies, particularly the weakness of informed consent in the educational environment, as well as the risks of profiling and data exploitation. Through the analysis of legal texts, the study concludes that traditional data protection laws are insufficient to address the predictive nature of artificial intelligence, which calls for urgent legislative reforms that incorporate the principle of privacy by design and guarantee the learner's right to digital forgetting.

Keywords: Artificial Intelligence, Personal Data, Learner Privacy, Informed Consent, Digital Forgetting.

Introduction:

The world is witnessing rapid technological transformations driven by artificial intelligence (AI) systems, whose impact has extended to various vital sectors, primarily the education sector. Technology is no longer limited to providing display tools or facilitating access to information; rather, it has become an active party in the education and evaluation processes through intelligent tutoring systems. These systems are characterized by their ability to track the learner's path, analyze their cognitive performance, and predict their educational difficulties, while providing customized educational content tailored to their needs. However, this development is accompanied by a massive expansion in the collection of learners' personal data, including their academic and behavioral data, which raises significant legal challenges related to the protection of the right to privacy.

Importance of the Research: The importance of this research lies in its focus on a legally and socially vulnerable group, namely the learner category, which includes minors and students. These individuals find themselves forced to use smart platforms as part of their mandatory educational path without having the luxury of refusal. Furthermore, its importance is evident in the attempt to bridge the gap between the rapid technical development in the field of educational technology in the Arab world and the stagnation that afflicts some national legislations regarding data protection.

Research Objectives: The research aims to achieve a set of objectives, most notably:

1. Determining the legal and technical nature of the data collected by artificial intelligence in the educational space.
2. Highlighting the risks resulting from the unlawful exploitation of learners' data.
3. Evaluating the efficiency of current legal rules in providing actual protection for learner privacy.
4. Proposing novel legal mechanisms that ensure a balance between the quality of digital education and the protection of rights.

Research Problem: The central problem of this research is embodied in the following fundamental question: To what extent does the current legal system provide effective protection for the learner's personal data against the deep and predictive processing mechanisms practiced by educational AI systems, and what are the legal guarantees that must be established to achieve a smart accompaniment environment that respects the right to privacy?

Research Hypothesis: The research proceeds from a fundamental hypothesis that traditional data protection legislation was not designed to keep pace with the algorithmic capabilities of artificial intelligence, and that the continuation of the legislative vacuum will inevitably lead to transforming the learner from the center of the educational process into a mere data commodity, which requires an exceptional legal framework.

Main Research Methods: To address the posed problem, the study relied on three main scientific methods that complemented each other to achieve a more accurate understanding of the research topic. The descriptive method was employed to present the nature of smart systems and explain their working mechanisms within educational environments, while clarifying the types of data they rely on in analyzing learners' behavior and personalizing learning paths. The analytical method was also used to deconstruct national and international legal texts related to data protection and regulating the use of AI technologies, aiming to reveal their limitations and their ability to respond to current technical shifts. In addition, the study adopted the comparative method to compare the trends of different legislations, especially between the European experience and some Arab legislations, in order to identify similarities and differences and anticipate the best regulatory practices that can be utilized in developing legal frameworks.

Research Divisions: To encompass all aspects of the topic, the research was divided into two sections. The first addresses the conceptual and technical framework for processing learner data via smart systems, and the second focuses on the legal mechanisms for protecting their privacy and their challenges.

Section One: The Conceptual and Technical Framework for Processing Learner Data via Smart Systems

A precise understanding of the nature of the technology used in the educational environment is a crucial first step in determining the legal scope of protection. AI technologies go beyond traditional archiving methods to reach the level of deep analysis and the deduction of behavioral patterns, which requires studying the type of data and the risks surrounding it.

Subsection One: The Nature of Personal Data Processed in the Smart Educational Environment

The contemporary educational environment is characterized by the abundance of data generated by learners' interactions with smart devices and platforms. Data is no longer limited to the name, date of birth, and grades, but has branched out to include the most minute details of the learner's cognitive and psychological activity.

Branch One: Academic and Behavioral Data

E-learning platforms integrated with artificial intelligence rely on real-time recording of all the learner's movements while using the software. This includes tracking the time a student spends reading a specific page, the number of times they rewatch a video clip, and answering patterns. This data, which seems purely academic, is transformed by machine learning algorithms into precise behavioral data reflecting the student's cognitive abilities and concentration level. This monitoring creates a cognitive footprint for the learner that is stored in cloud databases not always under the institution's control, but managed by intermediary companies. This flow is considered the raw material that feeds models to provide recommendations, keeping the learner under a constant digital microscope that records their slightest slips and interactions, and turns their behavior into numbers subject to continuous automated analysis and evaluation. ([1])

Behavioral data is not limited to academic interactions but extends to include social activity on campus in smart universities. Many institutions use smart cards and communication networks that record the student's movement path, their physical attendance rate, and the nature of the groups they mingle with. By merging this data with academic data, systems can build a comprehensive picture of the learner's personality and orientations. The legal danger here lies in the fact that this data may be used for purposes beyond the educational purpose, such as evaluating student discipline or predicting their likelihood of committing future violations. This expansion in data collection strips the educational process of its guiding character and turns it into social engineering controlled by algorithms, which constitutes a violation of the purpose limitation principle upon which data protection legislation in the world is based. ([2])

[1] -Al-Attiya Mahmoud, Artificial Intelligence in Education: Legal Opportunities and Challenges, (Amman: Dar Wael for Publishing, 2023), p. 45.

[2] - Abdul Rahman Salwa, "Legal Protection of Information in the Digital Age," Journal of Law and Political Sciences, Issue (3), Volume (12), (2022), p. 112.

Recent periods, especially in the year 2020 and beyond, have witnessed a surge in the use of exam surveillance systems. These systems rely heavily on the processing of learners' biometric data to verify their identity and prevent cheating. This includes the use of facial recognition technologies, iris analysis, voiceprint, and keystroke analysis, which is considered a unique kinetic signature. Collecting this type of data places us before an unprecedented level of interference in physical and moral sanctity, especially since biometric data is legally classified as highly sensitive data. The security justification often provided by institutions clashes with the difficulty of securing this data against breaches, in addition to the fact that algorithms have proven their shortcomings and bias against certain racial groups, leading to unjustified technological exclusion of students. ([3])

Alongside biometric data, a wave of AI systems has emerged claiming the ability to read the learner's emotional state by analyzing their facial expressions. This development represents a breakthrough into the last bastions of human privacy. From a legal standpoint, adapting this data to find out whether a student is feeling bored or stressed is considered a breach of freedom of thought and conscience. Transforming emotions into machine-readable data, and exploiting it to modify content, is often done without the student's true realization of the extent of the interference. The risks increase when these conclusions are linked to the final evaluation, where the learner is required to feign attention to satisfy the machine, which constitutes a blatant violation of their dignity and their right to a safe educational environment in the 21st century. ([4])

Graph No. (1): Types of Learner Data Processed by Algorithms

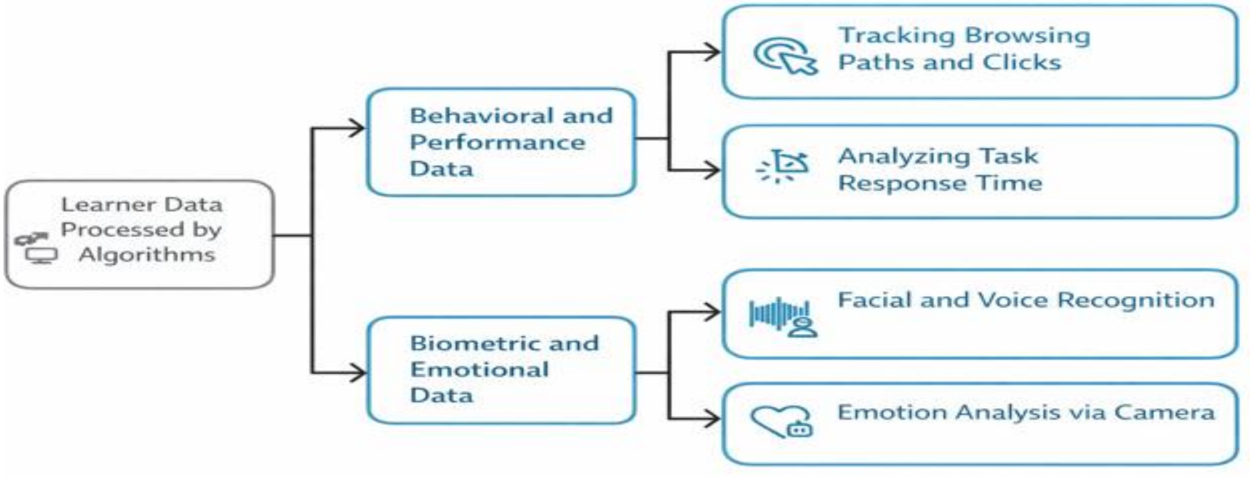
Learner Data Processed by Algorithms
Behavioral and Performance Data
Biometric and Emotional Data
Tracking Browsing Paths and Clicks
Analyzing Task Response Time
Facial and Voice Recognition
Emotion Analysis via Camera

Figure designed by the researcher

[3] -Al-Shammari Jassim, Legal Regulation of Biometric Data, (Kuwait: Kuwait University Publications, 2021), p. 88.

[4] -Mansour Tariq, "Emotional Artificial Intelligence and the Risks of Violating Private Life," Arab Journal of Legal Studies, Issue (1), Volume (5), (2024), p. 45.

Subsection Two: Risks Arising from the Unlawful Exploitation of Data

Accumulating this massive amount of data opens the door wide to risks that threaten the learner's future. Data in the digital age is the primary engine of the economy, and exploiting it outside the pure educational framework may turn technology into a tool for surveillance, discrimination, and systematic commercial exploitation.

Branch One: Profiling and Discriminatory Classification

Automated profiling and classification are among the most dangerous outcomes of using AI in education. Algorithms rely on classifying students into categories based on their previous performance, and perform predictive operations regarding their future level. This profiling leads to placing the learner in rigid molds that do not reflect the reality of their development. If the system classifies a student as a slow learner in their early stages, the algorithm may later withhold advanced content from them under the pretext that they will not comprehend it, which confiscates their right and limits their academic opportunities. This creates a closed cycle of frustration caused by the machine based on biased classifications, which contradicts the right to equality and equal opportunities in universities, and makes the learner a prisoner of their digital past. ([5])

In addition to restricting opportunities, smart profiling carries risks of social and racial discrimination. Systems are trained on historical data that carries human biases. When this system is applied in university orientation, it may exclude categories based on their residential areas deduced by the system. From a legal perspective, taking decisions that affect the learner's legal status, such as accepting or dismissing them based on purely automated processing without human intervention, is an explicit violation of human rights charters. The lack of transparency in the algorithmic black box prevents the learner from understanding the reasons for their exclusion, which strips them of their right to appeal and seek administrative review of decisions based on profiling, and threatens their professional path. ([6])

Branch Two: Commercial Exploitation and Cyber Breaches

The phenomenon of commodifying educational data represents a grave challenge to legislation. Many platforms that offer their services for free to schools collect learners' data to sell to targeted advertising companies or recruitment agencies. This exploitation takes place under vague licensing contracts whose details the student cannot comprehend. By virtue of this exploitation, the student transforms from a beneficiary of a service into a producer of data sold in data markets. As the researcher Al-Baz asserts in his study in 2022, "The legislator's silence

[5] -Ibrahim Mustafa, Algorithmic Governance and Human Rights, (Cairo: Dar Al-Nahda Al-Arabiya, 2022), p. 134.

[6] - Al-Bustani Nada, "Algorithmic Discrimination in Administrative Decisions," Journal of Law and Technology, Issue (2), Volume (8), (2023), p. 210.

regarding the commercial practices of educational companies is an abandonment of the security of future generations." The absence of deterrent texts preventing the trafficking of minors' data turns the right to privacy into mere ink on paper, and opens the field to targeting learners with advertisements specially designed to influence their convictions. ([7])

The danger does not stop at commercial exploitation but extends to cyber breaches. Educational institutions lack strong cybersecurity infrastructure, making their databases, which contain a treasure trove of information, a target for hackers. Leaking data that includes the psychological state and academic record of millions of students represents a social disaster. In the event of breaches, the legal system finds it difficult to clearly identify the responsible party: is it the institution as the controller, the programming company, or the cloud storage service provider? This fragmentation in civil liability and the failure to impose strict security measures on smart education platform contractors makes the learner the sole victim paying the price for cyber exposure. ([8])

Section Two: Legal Mechanisms for Protecting Learner Privacy and Their Challenges

Given the growing use of smart systems and their risks, it is necessary to examine the extent to which the legal arsenal responds to providing an effective umbrella of protection. Classic rules are no longer sufficient to respond to the challenges posed by artificial intelligence, which requires an exceptional adaptation of applicable principles.

Subsection One: The Inadequacy of General Rules and the Challenge of Informed Consent

Personal data protection laws, despite their development, are built on foundations designed at the beginning of the millennium and did not anticipate the predictive capabilities of artificial intelligence. The most prominent shortcoming is the legal adaptation of the principle of consent and approval, which is considered the cornerstone in the legality of processing.

Branch One: The Dilemma of Consent and Approval in the Educational Environment

The law in most countries of the world requires that consent to data processing be free and explicit. However, projecting this condition onto the educational environment reveals a structural flaw. In the relationship between the institution and the learner, equality is absent, and the learner falls into a subordinate and weak position. When a university decides to adopt a smart platform, the student is asked to click the agree button as a condition to access the platform. In this case, the student's consent cannot be described as free by any legal standard, but rather they represent contracts of adhesion. The student does not have the option to refuse without jeopardizing their

[7] -Al-Baz Abdullah, Privacy in the Era of Big Data, (Beirut: Arab Center for Research, 2022), p. 65.

[8] -Al-Sayegh Walid, "Cybersecurity in the Public Services Sector," Journal of Security Studies, Issue (4), Volume (15), (2021), p. 55.

future, which makes the condition of freedom in consent completely non-existent and a foregone conclusion. ([9])

On the other hand, the challenge of being informed in the granted consent emerges. Even if we assume the student's freedom, systems relying on deep learning algorithms operate in complex ways that not even their developers fully understand. So how can a student give consent based on knowledge of the nature of the outcomes that will result over their years of study? Privacy documents are drafted in complex legal and technical language, primarily aimed at absolving the company of liability. Amidst this complexity, obtaining the learner's consent becomes a mere formality with a legal cover, but internally it circumvents the person's right to actually control their data, which compels the legislator to search for alternative legal foundations. ([10])

Branch Two: The Responsiveness of National Laws to Artificial Intelligence

When analyzing legal texts in many countries in the Middle East and North Africa, we find that they have begun to grasp the importance of enacting legislation to protect data. However, these legislations came as a copy of general rules concerned with consumer data in the trade sector, and did not specify texts regulating processing by artificial intelligence in education. This absence leaves institutions floundering in interpreting general texts, as it is difficult to apply the restriction of the data retention period when the smart system needs that data to improve the accuracy of its algorithms. The inadequacy of texts is evident in their inability to address the issue of liability resulting from AI errors in academic evaluation, due to the lack of an explicit text regulating objections to automated decisions. ([11])

In contrast, the General Data Protection Regulation (GDPR), issued in 2016, constituted a precedent that attempted to address some shortcomings by establishing rights such as the right not to be subject to a decision based solely on automated processing. Despite the advancement of this framework, its application in the education sector faces practical obstacles. Therefore, national laws are currently demanded to move beyond the stage of general rules and move towards establishing sectoral regulation specific to educational technologies. This regulation must include strict requirements regarding the local localization of data, and not allowing the transfer of learners'

[9] -Mahmoud Hussam Al-Din, Electronic Consent in Technology Contracts, (Alexandria: Al-Halabi Legal Publications, 2019), p. 102.

[10] -Allam Yasser, "The Principle of Algorithmic Transparency in Modern Legislation," International Journal of Private Law, Issue (1), Volume (3), (2022), p. 89.

[11] -Al-Sharif Majid, Law and Emerging Technologies, (Riyadh: Law and Economics Library, 2023), p. 215.

data to foreign country servers, in order to protect digital sovereignty and prevent entire generations from falling under the surveillance of transcontinental corporations. ([12])

Graph (2): Challenges of Legal Protection for Learners' Data

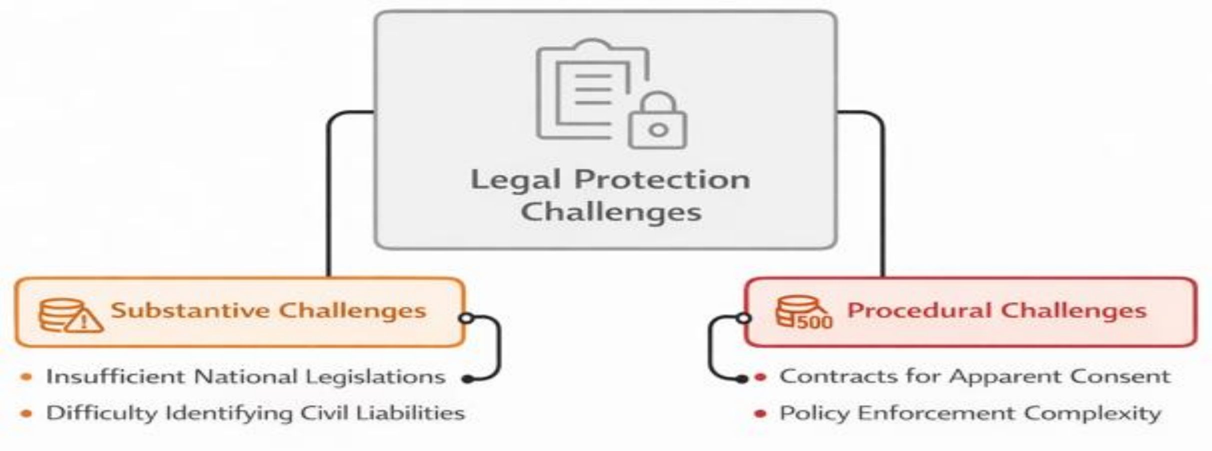
Legal Protection Challenges
Substantive Challenges
Insufficient National Legislations
Difficulty Identifying Civil Liabilities
500
Procedural Challenges
Contracts for Apparent Consent
Policy Enforcement Complexity

Figure designed by the researcher

Subsection Two: Towards Establishing Governing Principles for Intelligent Tutoring Systems

To rectify the deficit in traditional rules, legal jurisprudence turned to deducing proactive guiding principles that must govern the process of designing and deploying AI systems in education, ensuring the protection of privacy automatically and embedded within the technology itself.

Branch One: The Principle of Privacy by Design and Data Minimization

The principle of privacy by design is considered one of the most important modern solutions adopted to counter the encroachment of algorithms. This principle is based on the idea that protecting learner privacy should not be an afterthought to the data collection process, but must be integrated into the core code of the smart system from the very first moments of its design. In the educational field, this means that platforms must be designed so that their default settings are the most protective of the student, and they do not operate the camera, microphone, or location tracking except by explicit decision and for a limited period. This integration between law and programming lifts the burden of data protection off the learner's shoulders and places it on the manufacturing company, creating an educational environment that is structurally safe and impenetrable by its very composition. ([13])

[12]- Qasim Reem, "Cross-Border Transfer of Personal Data," Journal of International Law, Issue (2), Volume (9), (2021), p. 150.

[13] -Haroun Zakaria, Legal Engineering of Privacy, (Amman: Dar Al-Thaqafa, 2022), p. 118.

The principle of privacy by design is accompanied by another fundamental principle, which is data minimization. The voracious nature of artificial intelligence drives developers to collect everything possible under the pretext of improving service quality in the future. Legal intervention here must be decisive in enforcing a rule restricting data collection to what is deemed necessary to achieve the direct, pre-defined educational goal. For instance, if the system's purpose is to evaluate a student's answers in physics, there is no legal justification allowing the program to collect data about their geographical location or analyze their facial expressions. Institutions' commitment to applying the minimum standard reduces the volume of risks, and ensures that predictive operations remain confined to the academic scope. ([14])

Branch Two: The Learner's Right to Digital Forgetting

One of the most important newly established rights in the era of digitization, which gains double importance in education, is the right to digital forgetting. In traditional systems, the learner enjoyed the blessing of being forgotten, where their mistakes and behavioral slips were erased over time, and only their certificates and results remained. In the AI era, however, the digital memory of platforms never forgets; it retains every wrong answer and every academic stumble the student has made since their early years. The permanent storage of this behavioral data constitutes a heavy constraint on the individual's future, as it may be recalled later in employment stages to evaluate them based on an old stereotype that no longer represents them. Therefore, empowering the learner with the right to request the erasure of their educational footprint after graduating from university represents a legal and ethical necessity. ([15])

The practical application of the right to be forgotten in educational systems poses complex technical challenges. Companies claim that erasing a specific individual's data may weaken the accuracy of the algorithmic model. To confront this obstinacy, the legislator must intervene to compel institutions to adopt anonymization techniques from the beginning, so that algorithms benefit from general trends without linking them to the real identity of the student. When a student requests the erasure of their records, any link connecting the identity and the behavioral file must be destroyed permanently and irreversibly. Legally enshrining this right will restore the learner's control over their digital identity, and prevent schools from turning into surveillance institutions that produce lifelong archives imprisoning individuals in the mistakes of their past. ([16])

[14] -Salem Amina, "Principles of Data Processing in Smart Systems," Annals of Public Law, Issue (3), Volume (14), (2023), p. 95.

[15] -Al-Najjar Farid, The Right to be Forgotten in the Digital Environment, (Cairo: Dar Al-Fikr Al-Arabi, 2021), p. 67.

[16] -Al-Jabri Sanaa, "Challenges of Implementing the Right to Data Erasure," Journal of Contemporary Rights, Issue (1), Volume (11), (2022), p. 140.

Conclusion:

In conclusion, it is evident from this analytical study that the integration of artificial intelligence technologies into the educational system, despite its tremendous promises of improving learning quality and personalizing educational accompaniment, carries existential threats to the right to privacy and the protection of learners' personal data. The transformation of the student into an inexhaustible source of behavioral and biometric data, under systems that do not recognize the right to digital forgetting and operate with opaque algorithms, places the legislator before a real test to prove their ability to adapt technology to serve humans and not vice versa. The continuation of the legislative vacuum and the application of classic general rules will only lead to the entrenchment of a state of digital submission and the loss of sovereignty over personal identity.

At the conclusion of this study, a set of results and recommendations were reached that would contribute to strengthening the legal framework for data protection in the digital educational environment, ensuring a balance between employing AI technologies in developing the educational process on the one hand, and safeguarding learners' rights and privacy on the other.

First: Results: The research concluded with a set of results, the most important of which are:

1. The consent provided by the learner or their guardian to use educational platforms is considered superficial and adhesive due to the subordination to the institution.
2. Automated processing and algorithmic profiling of student behavior represent a direct threat to the principle of equal opportunity in institutions.
3. Current national data protection laws are characterized by generality and inadequacy in addressing the predictive nature of artificial intelligence.
4. The use of emotion analysis and biometric surveillance systems constitutes a serious infringement on human dignity.

Second: Recommendations: Based on the findings, we recommend the following:

1. The necessity of the legislator's intervention to issue precise sectoral regulatory texts that specifically govern data processing in the educational environment, given the sensitive nature of the data collected about learners inside educational institutions, such as academic, behavioral, and biometric data. This data requires a more specific legal framework than general data protection rules, ensuring the identification of authorized access entities, purposes of use, and retention periods, in addition to establishing clear safeguards to prevent its misuse or leakage.
2. The explicit legislative recognition of the learner's right to digital forgetting is an essential step to protect their privacy in the digital educational environment. This requires obligating educational institutions to delete or erase the digital and behavioral files of students after the end of their relationship with the institution, especially those related to learning patterns or behavioral assessments that may affect their future academic or professional opportunities, ensuring that no permanent digital trace remains that may limit the individual's freedom in building their future.

3. Imposing the principle of privacy by design as a fundamental condition in contracts for supplying software and educational platforms to schools and universities, so that data protection guarantees are integrated from the system design phase rather than after its operation. This includes minimizing data collection to the necessary minimum, encrypting it, defining access privileges, as well as ensuring transparency in how information is processed, thereby enhancing user trust and reducing risks associated with breaches or misuse.
4. Forming independent ethical and legal committees to audit algorithms and smart systems used in education before their approval or operation. The mission of these committees is to evaluate the extent of these systems' compliance with legal and ethical principles, especially concerning the prevention of algorithmic bias and ensuring fairness in educational evaluations, in addition to verifying the availability of sufficient standards for cybersecurity and data protection, thereby ensuring a responsible and safe use of AI technologies in the educational field.

Footnotes:

1. Al-Attiya, Mahmoud, Artificial Intelligence in Education: Legal Opportunities and Challenges, (Amman: Dar Wael for Publishing, 2023), p. 45.
2. Abdul Rahman, Salwa, "Legal Protection of Information in the Digital Age," Journal of Law and Political Sciences, Issue (3), Volume (12), (2022), p. 112.
3. Al-Shammari, Jassim, Legal Regulation of Biometric Data, (Kuwait: Kuwait University Publications, 2021), p. 88.
4. Mansour Tariq, "Emotional Artificial Intelligence and the Risks of Violating Private Life," Arab Journal of Legal Studies, Issue (1), Volume (5), (2024), p. 45.
5. Ibrahim Mustafa, Algorithmic Governance and Human Rights, (Cairo: Dar Al-Nahda Al-Arabiya, 2022), p. 134.
6. Al-Bustani Nada, "Algorithmic Discrimination in Administrative Decisions," Journal of Law and Technology, Issue (2), Volume (8), (2023), p. 210.
7. Al-Baz Abdullah, Privacy in the Era of Big Data, (Beirut: Arab Center for Research, 2022), p. 65.
8. Al-Sayegh Walid, "Cybersecurity in the Public Services Sector," Journal of Security Studies, Issue (4), Volume (15), (2021), p. 55.
9. Mahmoud Hussam Al-Din, Electronic Consent in Technology Contracts, (Alexandria: Al-Halabi Legal Publications, 2019), p. 102.
10. Allam Yasser, "The Principle of Algorithmic Transparency in Modern Legislation," International Journal of Private Law, Issue (1), Volume (3), (2022), p. 89.
11. Al-Sharif Majid, Law and Emerging Technologies, (Riyadh: Law and Economics Library, 2023), p. 215.
12. Qasim Reem, "Cross-Border Transfer of Personal Data," Journal of International Law, Issue (2), Volume (9), (2021), p. 150.
13. Haroun Zakaria, Legal Engineering of Privacy, (Amman: Dar Al-Thaqafa, 2022), p. 118.

14. Salem Amina, "Principles of Data Processing in Smart Systems," Annals of Public Law, Issue (3), Volume (14), (2023), p. 95.
15. (Al-Najjar), Farid, The Right to be Forgotten in the Digital Environment, (Cairo: Dar Al-Fikr Al-Arabi, 2021), p. 67.
16. Al-Jabri Sanaa, "Challenges of Implementing the Right to Data Erasure," Journal of Contemporary Rights, Issue (1), Volume (11), (2022), p. 140.