Uzbek Journal of Law and Digital Policy

Ethics of Automated Online Proctoring Balancing Academic Control with Students' Right to Privacy

Dilbar Suyunova,[1*]

[1] Tashkent State University of Law, Uzbekistan

* d.suyunova@tsul.uz

DECLARATIONS

Ethical Statement:

This research was conducted in accordance with the COPE Core Practices and principles of academic integrity, transparency, and responsible research.

Data Availability Statement:

Data supporting this study are available from the corresponding author upon reasonable request, where applicable.

AI Declaration:

The authors acknowledge the use of AI tools in conducting and preparing this research and remain fully responsible for its content, accuracy, and originality.

Conflict of Interest Statement:

The authors declare no conflicts of interest.

Funding Statement:

The authors received no funding for this research.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction provided the original work is properly cited.

Abstract

Automated online proctoring has become common across universities, including those in Uzbekistan, creating tension between academic integrity and student privacy. Institutions collect biometric, audio, and behavioral data during exams, often without clear legal boundaries or safeguards. This research examines whether Uzbekistan's Law on Personal Data adequately regulates such surveillance and proposes measures balancing institutional control with student rights. The study aims to identify privacy risks, evaluate legal adequacy, and recommend targeted reform for biometric exam data specifically. It uses qualitative doctrinal analysis, examining statutory text, legislative amendments, and scholarly literature through systematic document analysis. Results reveal persistent gaps: biometric vulnerability, algorithmic opacity, and unaddressed regulatory silence within current legislation. The study recommends a legislative amendment requiring mandatory impact assessment and separate informed consent before biometric proctoring deployment. Implementing this reform would strengthen legal protection, align Uzbekistan with international standards, and extend responsible governance into an under-regulated area of educational technology.

Keywords: Automated Online Proctoring, Personal Data Protection, Biometric Surveillance, Student Privacy Rights, Academic Integrity, Uzbekistan Data Protection Law, Legislative Amendment

How to Use Cite (APA 7th Edition)

Suyunova, D. (2026). Ethics of Automated Online Proctoring Balancing Academic Control with Students' Right to Privacy. *Uzbek Journal of Law and Digital Policy, 4*(5), 127-149. https://doi.org/10.59022/IRSHAD-ujldp.7

Authors Contribution:

Full.

I. INTRODUCTION

Universities now use automated software to watch students during online exams. These systems track eye movement, background sounds, and keyboard activity throughout the test. Proctoring companies promise fair exams and honest results for every learner. Yet this promise carries a hidden cost for personal privacy. Cameras record bedrooms, faces, and private conversations without full consent. Algorithms flag normal behavior as suspicious, causing stress and unfair penalties. Students with disabilities or unstable internet face harsher scrutiny under these systems. Many learners describe the process as invasive and deeply uncomfortable during assessments. Academic institutions defend these tools as necessary for protecting exam integrity. Still, few clear rules govern student data once proctoring software collects it. This gap raises a difficult question about control and dignity. Should academic honesty justify constant surveillance inside a student's private home? This paper examines that tension between institutional control and personal privacy (Khalil et al., 2022).

Online education expanded rapidly once campuses closed during global health emergencies. Universities needed a fast method to prevent cheating during remote assessments. Automated proctoring emerged as the preferred solution across many countries worldwide. These platforms combine facial recognition, screen recording, and behavior detection into one tool. Vendors market this technology as an objective substitute for exam supervisors. Institutions across Central Asia, including Uzbekistan, adopted similar remote testing arrangements quickly. Existing scholarship mostly examines proctoring within Western legal and educational systems. Fewer studies address how emerging data protection regimes apply to student surveillance. Uzbekistan’s Law on Personal Data regulates the collection and storage of citizen information. Its application to biometric exam data remains largely unexplored by researchers. Earlier work also treats academic integrity and privacy as separate concerns. This separation leaves a fragmented picture of the actual regulatory landscape. A combined legal and ethical view of proctoring practices is still missing (Coghlan et al., 2021).

Automated proctoring creates a direct conflict between exam security and personal privacy. Universities collect biometric data, video footage, and behavioral logs without transparent limits. Students rarely know how long this information stays stored after examinations end. Vendors sometimes share collected data with third parties for undisclosed commercial purposes. Current regulations struggle to classify exam surveillance data within existing privacy categories. Uzbekistan’s data protection framework was not designed with automated proctoring in mind. This mismatch leaves students without clear legal remedies for privacy violations. Institutions lack binding guidance on acceptable monitoring boundaries during assessments. The result is inconsistent practice across universities using similar proctoring software. Some schools disable microphones while others record continuous audio throughout exams. Students facing these varied rules cannot predict what privacy protection applies. This inconsistency shows an unresolved problem needing focused legal at-

tention. This research addresses that unresolved problem within Uzbekistan's higher education context (Han et al., 2024).

Recent scholarship documents growing concern over algorithmic bias within proctoring software. Archer examined how proctoring tools disproportionately affect students from marginalized backgrounds during exams. Her findings showed facial recognition errors increased anxiety among affected students significantly. Institutions using biased software risked violating principles of equal educational treatment. Her study also linked technical failures to broader questions about institutional accountability. These accountability gaps appeared across multiple universities regardless of national location. Researchers increasingly argue that technical fixes alone cannot resolve fairness concerns. Policy frameworks must address bias alongside privacy protections within proctoring regulations. This finding strengthens the case for combined ethical and legal analysis. Without such analysis, universities may continue relying on flawed monitoring systems. Bias therefore remains a pressing concern within current academic integrity practices. Institutions adopting new software rarely test these tools for demographic fairness beforehand. Vendors also publish limited data explaining how detection algorithms actually operate internally (Archer, 2023).

Maphalala and Nosy studied proctoring within open distance learning environments across developing regions. Their research found students accepted monitoring when institutions explained data handling clearly. Transparency reduced anxiety and improved perceived fairness of automated exam supervision. Students without reliable internet access still faced unfair suspicion flags regularly. Their study recommended clearer institutional policies alongside improved technical infrastructure support. This finding highlights infrastructure inequality as a hidden dimension of proctoring ethics. Few studies connect infrastructure gaps directly to data protection law compliance. This combined perspective remains largely absent from proctoring literature focused on wealthier regions. Uzbekistan’s developing digital infrastructure makes this connection especially relevant for local policy. These insights guide the present study’s focus on regulatory and practical gaps. Together, both studies show fairness depends on technology, policy, and infrastructure combined. Neither study, though, examines a specific national data protection statute in depth (Maphalala & Nkosi, 2025).

Existing literature separately examines technical bias, student experience, and general data protection principles. Few studies connect these three areas within a single coherent legal framework. Research on proctoring rarely engages directly with Central Asian data protection statutes. Uzbekistan’s Law on Personal Data has not been tested against biometric exam surveillance. Scholars studying academic integrity technology often overlook specific regional legal contexts entirely. This creates a gap between global ethical debates and local regulatory realities. Future research directions mentioned in existing studies call for jurisdiction-specific legal analysis. No published work currently applies Uzbekistan’s privacy statute to proctoring practices directly. Prior studies also focus mainly on higher education systems in wealthier nations. Developing economies with expanding digital education sectors receive comparatively little scholarly attention. This research fills that specific

gap through focused legal and ethical analysis. It connects international proctoring debates to Uzbekistan's developing data protection framework directly (Heinrich, 2025).

To examine the privacy risks created by automated online proctoring systems in higher education.

To assess whether Uzbekistan's Law on Personal Data adequately regulates biometric exam surveillance data.

To propose legal and institutional measures balancing academic integrity with student privacy rights.

How can Uzbekistan's data protection framework be strengthened to balance academic integrity with students' right to privacy during automated online proctoring?

Automated proctoring will likely remain standard practice across universities for years ahead. Without clear regulation, students face continued exposure to invasive and unfair surveillance practices. Uzbekistan’s growing digital education sector needs proactive legal guidance before problems escalate further. Addressing this issue now prevents costly legal disputes and reputational harm for institutions. Universities also benefit from clear compliance standards that reduce inconsistent monitoring practices. Students deserve confidence that assessment technology respects their fundamental privacy rights. Policymakers require evidence-based recommendations grounded in current international scholarship and local law. This research provides that evidence through combined legal and ethical examination. Its timing matches Uzbekistan’s ongoing efforts to modernize personal data protection legislation. Delaying such analysis risks embedding flawed proctoring practices into permanent institutional policy. Regional universities also need a reference framework as proctoring adoption continues expanding. The findings can directly inform upcoming regulatory or institutional policy decisions (Malhotra, 2026).

II. METHODS & METHODOLOGY

This research applies qualitative research methods appropriate for legal and policy analysis. Doctrinal legal analysis forms the core methodological approach throughout this entire study. This method examines statutory text, legislative amendments, and official government sources directly. It suits research questions asking what a law requires and where gaps exist. Quantitative survey methods were not used, since this study analyzes existing legal text. The target population consists of Uzbekistan’s personal data protection legislation and related regulations. The specific sample examined is the Law on Personal Data, Act No. ZRU-547, alongside its 2021 and 2026 amendments. This narrow sample allows detailed, focused analysis rather than broad, shallow comparison. Document analysis complements doctrinal analysis by examining scholarly commentary and secondary legal literature. Together these methods let the research trace both formal legal text and expert interpretation. This combination suits a study proposing a specific, targeted statutory amendment. The approach remains consistent with standard practice across contemporary legal research.

Data collection relied on two main source categories: primary legislation and scholarly literature. Primary legal sources, including the Law on Personal Data, were obtained through Uzbekistan's official legislation portal, lex.uz. Presidential decrees and Cabinet resolutions were verified through official government publication channels wherever possible. Scholarly sources were retrieved using targeted keyword searches across academic databases and repositories. Keywords included personal data protection, biometric surveillance, automated proctoring, Uzbekistan data law, and related terms. Databases searched included Zenodo, Cyberleninka, and journal platforms publishing Central Asian legal scholarship. Searches prioritized peer-reviewed journal articles, book chapters, and dissertation-level legal monographs specifically. Inclusion criteria required direct relevance to personal data law, education technology, or comparable regulatory frameworks. Sources lacking identifiable individual authorship were generally excluded from formal citation within this research. This selective approach ensured traceable, verifiable sources throughout the entire analysis. Combining official legal text with scholarly commentary produced a well-grounded evidentiary foundation.

Validity and reliability were maintained by prioritizing recent scholarship, generally published within the last five years. Older sources were included only when addressing foundational concepts still relevant today directly. Currently applicable law versions were checked against the most recent legislative amendments available. This step ensured analysis reflected Uzbekistan’s present legal framework rather than outdated provisions. Ethical considerations required using only publicly available official documents throughout the entire research process. Every scholarly source consulted receives full in-text citation and complete bibliographic reference. No private, confidential, or restricted-access material was used at any research stage. This research also acknowledges clear limitations tied to its subject matter's evolving nature. Technology, particularly automated proctoring, continues changing rapidly across different institutional and vendor contexts. Personal data legislation in Uzbekistan can likewise be amended without extensive advance notice. Findings therefore reflect the legal and technological landscape as understood at research completion. Future legislative or technological developments may require corresponding updates to this analysis.

III. RESULTS& FINDINGS

This section presents results addressing ethics within automated online proctoring systems. It focuses on balancing academic control with students' right to privacy. Findings respond directly to the objectives guiding this research study. These objectives examined privacy risks, legal adequacy, and possible institutional reform measures. The results also answer the central question about strengthening Uzbekistan’s data protection framework. Each finding highlights a distinct dimension of the privacy and integrity conflict. Together they reveal how biometric collection, algorithmic opacity, and weak policy interact. Recent stakeholder research confirms that awareness and responsibility remain unevenly distributed across institutions. Universities, vendors, and students often hold different under-

standings of acceptable monitoring practices. This divergence shapes how proctoring risks manifest within specific educational and legal contexts. The following results synthesize legal analysis with recent scholarship on stakeholder perception. They provide the evidentiary foundation for the discussion and recommendations presented later. Readers should keep these interconnected findings in mind throughout the sections ahead (Mutimukwe, 2026).

Further findings show that student experience adds another layer to this vulnerability. Scoping reviews of remote proctoring describe consistent discomfort reported by test-takers worldwide. Students frequently mention feeling watched inside spaces meant to remain private. Bedrooms, kitchens, and shared living areas become visible to unknown proctoring staff. This exposure blurs the line between academic assessment and personal domestic life. Many students report reduced concentration caused by constant awareness of camera surveillance. Some describe symptoms resembling exam anxiety intensified specifically by monitoring technology itself. Reviewers note that institutions rarely measure these psychological effects before deploying proctoring tools. Without such measurement, universities cannot claim their systems protect student wellbeing adequately. This evidence strengthens the case that students function as vulnerable data subjects throughout. Their vulnerability extends beyond legal categories into everyday lived examination experience directly. Institutions should treat this lived experience as direct evidence supporting stronger legal protection (Marano et al., 2024).

Additional findings connect this opacity to broader failures in respecting contextual privacy norms. Students share personal spaces and behaviors expecting information to stay within academic boundaries. Proctoring systems collect data flowing far beyond what students reasonably anticipate during enrollment. Scoping research describes this mismatch using the framework of contextual integrity violation. Data gathered for exam supervision frequently moves to vendors, servers, and undisclosed third parties. Students rarely learn which specific actors eventually access their recorded exam sessions. This unclear data flow compounds the accountability problem already identified within these systems. Reviewers recommend treating each new data flow as a distinct integrity concern requiring justification. Institutions adopting proctoring rarely conduct this contextual assessment before implementation begins. The absence of such assessment leaves students unable to anticipate how their data travels. Addressing this requires the same reviewable accountability structures already proposed within this research. Regulators should therefore require contextual privacy assessments alongside routine data protection reviews (Mutimukwe et al., 2023).

IV. DISCUSSION & ANALYSES

A. Justification for the Proposed Amendment to Uzbekistan's Law on Personal Data

Uzbekistan adopted the Law on Personal Data through Act No. ZRU-547 in 2019. This law created the first structured framework for citizen data protection nationally. It defines personal data, sets processing rules, and assigns institutional oversight duties. The statute was written before automated proctoring became common in universities. It therefore con-

tains no specific rules addressing biometric exam surveillance directly. Students taking proctored exams now generate facial, audio, and behavioral data constantly. None of this data receives treatment matching its sensitivity under current provisions. The proposed amendment aims to close this specific and growing regulatory gap. It would require institutions to assess risks before deploying biometric proctoring tools. It would also require documented consent separate from ordinary enrollment paperwork. This purpose directly supports balancing academic control with genuine student privacy protection. The amendment therefore extends the law's original intent into a new technological context. Its purpose is protective, targeted, and consistent with the law's founding legislative goals (AllahRakha, 2024).

Recent legislative reform confirms Uzbekistan continues refining its personal data protection approach actively. In 2026, lawmakers relaxed general data localization rules to support economic growth. Most personal data may now move across borders under specified legal conditions. Biometric and genetic data remain subject to strict local storage requirements still. Lawmakers therefore already treat biometric information as deserving heightened protection compared to other data. This distinction directly supports extending similar heightened treatment to proctoring-collected biometric records. The proposed amendment simply applies this existing legislative logic to a specific educational context. It does not introduce an unfamiliar concept into Uzbekistan’s regulatory tradition at all. Empirical research on digital platforms confirms that regulatory effectiveness depends on targeted, sector-specific rules. General consent mechanisms alone rarely produce meaningful privacy protection for sensitive data categories. The amendment therefore follows an approach already validated within recent national policy practice. It builds directly on the legislature's own recognition of biometric data sensitivity (Otaboyev, 2026).

Scholarly case studies of Uzbekistan’s Personal Data Law reveal persistent enforcement and coverage gaps. Comparative research describes strong formal rights alongside weaker practical implementation across many sectors nationally. Education technology exemplifies this pattern, since no dedicated proctoring provisions currently exist anywhere. Universities therefore interpret general consent and processing rules without clear sector-specific guidance available. This uncertainty produces inconsistent practices across institutions using similar automated proctoring technology. Some universities disable data-sharing features while others rely entirely on vendor default settings. Such inconsistency undermines the law's broader goal of predictable, enforceable data protection nationwide. The proposed amendment would close this specific implementation gap within higher education directly. It would give universities concrete, sector-specific obligations rather than vague general principles alone. Students would similarly gain predictable protections instead of inconsistent institutional treatment nationwide. This alignment between formal law and practical enforcement strengthens the case for reform. Closing implementation gaps remains central to improving Uzbekistan’s data protection performance nationally (Yusupova & Ergashev, 2024).

Comparative legal analysis situates Uzbekistan's framework between older regional models and emerging international standards. The 2019 law and later constitutional provisions formally guarantee core data subject rights clearly. These rights include consent, access, and protection against unauthorized data processing generally. Yet comparative scholarship notes several distinctive gaps separating Uzbekistan's model from fuller international frameworks. Missing sector-specific rules for education technology represent one clearly identified gap needing attention. The proposed amendment directly addresses this identified gap within the comparative legal literature. It brings Uzbekistan's proctoring practices closer to standards already expected internationally elsewhere. Doing so would strengthen Uzbekistan's alignment with recognized international data protection principles significantly. Universities would operate under rules comparable to institutions in more developed regulatory environments. Students would receive protection consistent with international expectations rather than falling behind them. This alignment supports the amendment's broader goal of balancing control and privacy fairly. Comparative legal development therefore provides strong external justification for adopting this specific reform (Makhkamova, 2025).

The original Law on Personal Data was framed around reinforcing citizens fundamental privacy rights. Its provisions reflect a clear intention to protect individuals from unchecked data collection. Extending these protections into automated proctoring honors that original legislative purpose faithfully. Cyber law scholarship emphasizes those safeguarding digital spaces and personal data effectively. Effective safeguarding requires updating legal instruments as new digital practices continue emerging constantly. Automated proctoring exemplifies exactly the kind of practice such scholarship warns about. Without targeted rules, personal data protection remains theoretical rather than practically enforceable. The proposed amendment converts theoretical protection into practical, enforceable institutional obligations directly. It ensures cyberspace protections extend meaningfully into everyday educational digital environments. This connection between founding legislative intent and practical application strengthens the amendment's justification. Legal continuity, rather than disruption, characterizes this proposed regulatory addition. Students gain protection while institutions retain the ability to conduct fair, secure assessments (Rakha, 2023).

Placing Uzbekistan within its regional context clarifies why this amendment matters significantly now. Data privacy laws across Central Asia often balance domestic control with global standards. Uzbekistan's framework has been described as positioned between older regional models and newer international influences. This positioning creates opportunity for targeted, forward-looking legal improvements like the proposed amendment. Neighboring approaches to digital governance rarely include detailed education technology provisions either. Uzbekistan could therefore establish regional leadership by adopting clear proctoring safeguards first. Such leadership would strengthen the country's reputation within broader digital governance discussions. It would also provide a practical model for neighboring states facing similar challenges. Regional comparison shows most frameworks still lack sector-specific biometric exam protections generally. This gap represents both a

shared regional problem and a genuine improvement opportunity. The proposed amendment positions Uzbekistan ahead of comparable regional data protection developments. Regional leadership of this kind carries both symbolic and practical policy value (Greenleaf, 2025).

Digital transformation continues reshaping how human rights protections apply within everyday institutional practice. Scholarship on this evolution highlights growing tension between technological convenience and individual rights. Automated proctoring illustrates this tension clearly within the higher education sector specifically. Students privacy rights deserve protection equal to protections offered in other digital contexts. The proposed amendment operationalizes human rights principles within a concrete institutional setting directly. It ensures technological convenience for universities does not override fundamental student privacy interests. This balance reflects broader legal evolution connecting digital transformation with sustained rights protection. Human rights frameworks provide the underlying justification for every specific safeguard proposed here. Impact assessments and informed consent both trace back to core rights-based reasoning. Adopting this amendment would demonstrate practical commitment to that evolving rights framework. It would confirm that legal modernization and human rights protection can advance together. This final justification completes the case for the proposed legislative amendment (Akmal, 2025).

B. How the Proposed Amendment Differs from the Current Law on Personal Data (No. ZRU-547)

The current Law on Personal Data covers all forms of citizen information broadly. It applies equally to financial records, medical files, and general online activity. Recent scholarship notes that biometric, genetic, and behavioral data now demand separate treatment. Artificial intelligence systems process these categories differently from ordinary administrative records today. The current statute does not distinguish automated exam monitoring from routine data collection. This general design leaves proctoring technology without any dedicated regulatory attention whatsoever. The proposed amendment changes this by targeting one specific high-risk activity directly. It applies only where universities deploy biometric surveillance during examination periods. This narrower scope allows more precise obligations than the current general framework provides. General laws struggle to address fast-moving educational technology with sufficient detail. A sector-specific addition captures risks that broad legislation naturally overlooks entirely. This distinction represents the amendment's most fundamental departure from existing legal structure. It reflects a shift from general regulation toward focused, technology-specific legal design (Anorboev, 2026).

Current law relies mainly on a general consent model for lawful data processing. Institutions collect consent once, often during enrollment, covering broad future data use. This single-step approach works reasonably well for routine administrative record keeping. It performs poorly when applied to continuous biometric monitoring during examinations. Recent research identifies weak enforcement mechanisms as a persistent problem within current practice. Institutions face few concrete obligations beyond obtaining initial, general

consent from students. The proposed amendment introduces a mandatory data protection impact assessment before deployment begins. This assessment requires evaluating necessity, proportionality, and safeguards for each specific proctoring system. No equivalent requirement exists anywhere within the current legal text today. Consent under the amendment must also be separate, specific, and clearly documented. This differs sharply from bundled consent buried within standard enrollment paperwork. The amendment therefore introduces procedural rigor absent from the law's original consent approach (Yuldashev, 2024).

Localization rules form another area where the amendment differs from current legal provisions. Recent legislative changes already require strict local storage specifically for biometric and genetic data. This shows lawmakers recognize biometric information as uniquely sensitive within broader personal data categories. Localization alone does not regulate how universities collect that data initially. It addresses storage location without addressing consent, necessity, or institutional accountability directly. The proposed amendment complements localization by regulating the collection process itself specifically. It requires justification before biometric proctoring begins, not only secure storage afterward. This creates a fuller protection cycle covering collection, assessment, consent, and storage together. Current law only strongly regulates the final storage stage of this cycle. The amendment therefore closes a procedural gap that localization requirements alone cannot address. Together, both provisions would offer more complete protection than either provides separately. The amendment therefore builds naturally on existing legislative momentum rather than starting anew (AllahRakha, 2024).

Information security concerns shape much of Uzbekistan’s current personal data legislation broadly. National security and system protection often receive stronger emphasis than individual student experience. Scholarship on digital-era information security highlights this institutional and national security orientation clearly. Universities implementing proctoring technology currently focus primarily on preventing external cyber attacks and breaches. Less attention goes toward protecting students from the surveillance system's everyday operation itself. The proposed amendment shifts some focus toward this overlooked individual experience dimension directly. It requires institutions to consider psychological and educational effects, not only technical security risks. This complements existing security-focused provisions rather than replacing their continued institutional importance. Both security and individual protection can coexist within a single strengthened legal framework. The amendment therefore broadens the law's protective scope beyond narrow technical security concerns. This shift reflects growing international recognition that security and privacy require joint, coordinated attention (Sagymbaev, 2026).

Current law grants students reactive rights, including correction and deletion of inaccurate personal data. Students can request removal only after problematic data already exists within institutional systems. This reactive structure assumes harm becomes visible only once data processing has already occurred. Proctoring technology creates continuous, real-time surveillance during the examination itself. Waiting for after-the-fact correction offers little protection against surveillance-related harm happening immediately. The pro-

posed amendment introduces a proactive requirement through mandatory pre-deployment impact assessment. Institutions must evaluate risks before students ever face biometric exam surveillance directly. This shifts protection earlier in the process, preventing harm rather than merely correcting it. Existing deletion rights remain valuable but insufficient for real-time monitoring technology specifically. The amendment therefore adds anticipatory protection that current reactive rights alone cannot reasonably provide. Combining reactive and proactive tools gives students meaningfully stronger, more complete legal protection (Vapayev, 2023).

Comparative analysis shows Uzbekistan's current law lags behind more developed international data protection frameworks. Formal rights exist on paper but often lack detailed implementation guidance for specific sectors. Education technology represents one area where this comparative gap becomes especially visible today. Countries with stronger frameworks typically include sector-specific rules for sensitive processing activities directly. Uzbekistan's current law contains no equivalent provision addressing automated examination surveillance specifically. The proposed amendment would narrow this comparative gap by adding targeted sector regulation. It brings Uzbekistan's legal framework closer to practices already established internationally elsewhere. This improvement strengthens the country's broader reputation within global data protection discussions. Universities would also benefit from clearer guidance matching international institutional compliance expectations more closely. Students would receive protection comparable to peers studying under stronger foreign frameworks. This comparative improvement represents a concrete, measurable difference from the current, unlamented legal text (Khodzhanova, 2024).

The current law protects personal life inviolability through general civil regulation principles broadly. These principles cover housing privacy, personal identity, and protection of private communications generally. They were not written with specific attention toward educational examination environments directly. Proctoring technology places cameras and microphones inside deeply personal spaces during exams. This creates tension between general privacy principles and a genuinely new surveillance context. The proposed amendment extends established privacy principles into this previously unaddressed educational domain specifically. It applies familiar legal values to circumstances the original drafters never anticipated fully. This extension respects existing legal tradition while responding to modern technological reality directly. The current law's strength lies in general principle; the amendment's strength lies in application. Together they would form a more complete privacy protection system for students. This combination represents the clearest practical difference between the existing law and the proposed reform (Koryog'diyev, 2023).

C. Challenges to Applying the Law on Personal Data (No. ZRU-547)

Applying the Law on Personal Data faces a basic institutional stability challenge nationwide. The original regulator, the State Personalization Centre, no longer exists in its earlier form. Administrative reform moved oversight into a new Personalization Agency under the Ministry of Justice. Such structural change can disrupt ongoing investigations, guidance is-

suance, and institutional memory temporarily. Businesses must track which authority currently holds jurisdiction over their compliance obligations. Frequent institutional reshuffling makes long-term regulatory planning genuinely difficult for smaller organizations especially. Recent research on compliance mechanisms highlights how institutional instability weakens enforcement consistency broadly. Clear authority matters because unclear jurisdiction delays complaint handling and violation response significantly. Universities deploying proctoring technology need one stable point of regulatory contact reliably. Constant reorganization complicates that need considerably during a period of rapid technological adoption. This institutional challenge sits beneath many other specific implementation problems discussed throughout this section. Stability, not just good rules, determines whether legal protection actually reaches affected students (Khidirova, 2026).

Public awareness of personal data concepts remains another significant obstacle to effective application. Many citizens cannot clearly distinguish ordinary information from legally protected personal data categories. This confusion weakens the consent process, since informed consent requires genuine conceptual clarity first. Scholarship on personal data definitions notes persistent gaps between legal terminology and public comprehension. Students asked to consent to proctoring surveillance may not grasp what biometric data actually means. Without this basic clarity, consent risks becoming a formality rather than genuine agreement. Universities rarely invest time explaining these concepts clearly before collecting sensitive examination data. This gap between legal definition and everyday comprehension undermines the law's protective intention significantly. Strengthening public data literacy would improve compliance far beyond simple legal enforcement alone. Education about personal data concepts should accompany any new proctoring-specific regulatory requirement introduced. Otherwise, formal legal rights remain theoretical rather than practically exercised by ordinary students. This challenge affects implementation across nearly every sector, not only higher education institutions (Xushvaqtova, 2024).

Technical and linguistic capacity presents a further challenge to consistent legal application nationwide. Much international guidance on data protection and information security circulates primarily in English. Recent research highlights English proficiency as increasingly important for advancing national information security practice. Compliance officers reviewing vendor contracts often need fluent technical English for proctoring software agreements. Universities negotiating with international proctoring vendors face documentation written entirely in foreign legal language. Misunderstanding technical terms can lead to weak contracts that fail to protect student data adequately. Smaller institutions particularly struggle to access qualified staff combining legal, technical, and language skills together. This capacity gap slows accurate implementation of otherwise well-intentioned legal requirements significantly. Building specialized training programs could help close this practical implementation gap over time. Until then, language and technical capacity remain quiet but genuine barriers to compliance. Addressing this gap deserves attention alongside more visible legislative and institutional reform efforts (Muhammadjonova, 2025).

Rapid digital transformation creates a moving target that legislation struggles to track consistently. New technologies, including automated proctoring, emerge faster than dedicated legal provisions can be drafted. Research on Uzbekistan's digitalization process describes law consistently catching up rather than proactively anticipating change. This lag creates temporary regulatory gaps whenever genuinely new technology enters widespread institutional use. Universities adopting proctoring tools today operate within rules designed before such technology existed. Coordinating updates across multiple overlapping decrees, resolutions, and the core law itself proves administratively complex. Different institutions sometimes apply inconsistent interpretations while waiting for clearer, updated guidance to arrive. This coordination challenge affects not only education but nearly every rapidly digitalizing economic sector. Addressing it requires faster legislative response mechanisms alongside the specific amendment proposed here. Without such mechanisms, new technologies will keep outpacing available legal protection repeatedly. This structural lag represents a genuine, recurring challenge rather than a one-time implementation problem (Amaniyazova, 2023).

Vulnerable groups face particular difficulty navigating personal data protections within the current digital environment. Students, especially those unfamiliar with technology, may struggle to exercise their formal legal rights. Research on digital-era personal data protection notes that awareness alone does not guarantee genuine protection. Practical barriers, including unclear complaint procedures, discourage students from challenging problematic proctoring practices directly. Fear of academic consequences may also discourage students from raising concerns about surveillance practices openly. This power imbalance between students and universities complicates straightforward legal rights exercise considerably. Formal consent mechanisms cannot fully compensate for these underlying practical and psychological barriers alone. Institutions rarely provide accessible, confidential channels specifically designed for surveillance-related student complaints currently. Building such channels would meaningfully strengthen practical application of existing legal protections significantly. Without them, formal rights risk remaining largely theoretical for the students who need protection most. This challenge connects directly to broader questions about power and vulnerability within educational institutions (Eshdavlatova, 2022).

Aligning constitutional privacy guarantees with everyday institutional practice presents another significant implementation challenge. The Constitution guarantees inviolability of private life as a fundamental citizen right broadly. Recent scholarship examines how well ordinary legislation translates these constitutional guarantees into enforceable everyday protection. Gaps sometimes appear between constitutional aspiration and the specific, technical rules institutions actually follow. Proctoring technology tests this alignment directly, since it involves deeply personal spaces and behavior. Universities must interpret general constitutional privacy language when designing specific proctoring policies internally. Without clear statutory guidance, institutions risk inconsistent, sometimes constitutionally questionable, interpretations of their obligations. Strengthening the connection between constitutional principle and specific technological regulation would reduce this

uncertainty. The proposed amendment offers one concrete way to close this particular alignment gap. Doing so would help ensure proctoring practices genuinely reflect constitutional privacy commitments, not merely reference them. This alignment challenge illustrates why sector-specific rules matter alongside strong general constitutional protection (Baxodirov, 2026).

Recent enforcement reforms illustrate both progress and continuing difficulty applying the law consistently. A 2025 presidential decree introduced compulsory breach notification and clearer liability for the financial sector specifically. This reform shows government willingness to strengthen practical accountability beyond general declarative legal principles. Similar sector-specific enforcement mechanisms do not yet exist for higher education institutions. Universities currently face vaguer accountability standards than banks now operating under updated financial sector rules. This uneven development creates inconsistent protection depending entirely on which sector a student or customer occupies. Extending comparable breach notification and liability standards to education would address this inconsistency directly. The proposed amendment's impact assessment requirement moves toward this same enforcement clarity for universities. Without such extension, sensitive sectors like education remain comparatively under-regulated despite handling equally sensitive data. Recent financial sector reform therefore provides both a model and a challenge for future reform. Closing this cross-sector gap remains essential for genuinely consistent nationwide legal application (Ollaberganov, 2026).

D. Recommendations for Implementing the Amendment and the Law on Personal Data (No. ZRU-547)

The first recommendation is straightforward adoption of the proposed amendment into formal legislation. Uzbekistan's Digital Uzbekistan 2030 strategy already commits the country to responsible digital governance nationwide. Embedding proctoring-specific rules within the Law on Personal Data fits naturally within this strategy. Parliament should schedule the amendment for review alongside other ongoing digital governance legislative updates. Early adoption signals clear commitment before proctoring technology becomes even more widespread nationally. Delaying reform risks entrenching current gaps as more universities adopt biometric exam surveillance. Lawmakers should consult universities, students, and technology vendors before finalizing the amendment's exact wording. Broad consultation improves both legitimacy and practical workability of any new legal requirement. The Ministry of Higher Education should coordinate this consultation alongside the Ministry of Justice directly. Clear timelines and implementation deadlines should accompany the amendment once formally adopted. This structured approach turns the proposal from academic recommendation into genuine, actionable legal reform (Nyssankuatova et al., 2026)

Universities need dedicated training programs preparing staff to implement new proctoring-specific data protection requirements. Current cyber security scholarship on Uzbekistan highlights persistent skill gaps within many public institutions nationally. Training

should cover impact assessment methodology, consent design, and basic biometric data handling principles. Designated data protection officers at each university would anchor this new institutional responsibility clearly. These officers should receive specialized preparation before proctoring impact assessments become mandatory under the amendment. International organizations already support similar capacity-building programs across other Central Asian digital governance initiatives. Uzbekistan could adapt these existing programs specifically for higher education data protection needs. Universities lacking resources for full-time officers could share expertise through regional training consortiums instead. This collaborative model reduces cost while still building necessary specialized institutional knowledge nationwide. Without trained personnel, even well-written legal requirements risk poor, inconsistent practical implementation. Investing in people, not only legal text, determines whether this reform genuinely succeeds (Abdullaeva et al., 2023).

Universities and vendors should adopt privacy-by-design principles when building or selecting proctoring technology. This approach embeds data protection into system design rather than adding it afterward. Foundational privacy scholarship describes embedding protection throughout a technology's entire operational lifecycle directly. Applied to proctoring, this means collecting only data strictly necessary for exam integrity purposes. Systems should default toward minimal monitoring rather than maximal surveillance unless clearly justified otherwise. Procurement contracts should require vendors to demonstrate privacy-by-design compliance before universities approve their software. This shifts responsibility partly onto vendors, encouraging better privacy practices across the broader proctoring technology market. Universities gain leverage by making privacy-by-design a standard procurement requirement rather than an optional preference. Over time, this market pressure could improve proctoring technology more broadly across the region. The proposed amendment’s impact assessment requirement naturally encourages this privacy-by-design procurement approach directly. Combining legal requirement with market incentive strengthens the reform's practical effectiveness considerably (Cavoukian, 2009).

Regulators drafting detailed implementation guidance should use established privacy taxonomies to categorize specific proctoring harms. Classic privacy scholarship identifies distinct harm categories, including surveillance, exposure, and unwanted disclosure separately. Applying this framework helps universities recognize which specific risks their proctoring systems actually create. Surveillance harm covers continuous monitoring during exams; exposure harm covers footage viewed by unauthorized staff. Distinguishing these categories allows more precise, targeted safeguards rather than vague general precautions alone. Implementation guidelines could require universities to address each identified harm category within their impact assessments specifically. This structured approach makes required assessments more rigorous and genuinely useful for identifying gaps. Regulators could publish a standard checklist based on this taxonomy for universities to follow consistently. Consistency across institutions would also make later regulatory review and enforcement considerably more straightforward. Precise harm categorization turns abstract privacy principles into concrete, actionable institutional practice (Solove, 2006).

Consent mechanisms require complete redesign based on established research into genuine privacy-related decision-making behavior. Research shows people frequently accept privacy terms without fully processing what those terms actually permit. Applied to proctoring, universities should present consent requests separately from bundled enrollment documentation entirely. Clear, plain-language explanations should accompany each consent request, avoiding dense legal or technical wording. Students should receive genuine opportunity to ask questions before confirming consent to biometric surveillance. Consent interfaces should avoid design patterns that subtly pressure students toward automatic, uninformed acceptance. Behavioral privacy research consistently shows interface design meaningfully shapes how freely people actually consent. Universities implementing the proposed amendment should test consent interfaces for genuine clarity before full deployment. Student feedback during this testing phase would help identify confusing or misleading consent language early. Well-designed consent processes protect both students and universities from later disputes about genuine agreement (Acquisti et al., 2022).

Universities should establish interdisciplinary review boards combining legal, technical, and educational expertise before approving proctoring deployments. Broader privacy scholarship recommends exactly this interdisciplinary approach for evaluating complex, technology-driven decisions responsibly. A single department, whether legal or technical alone, rarely captures every relevant risk dimension. Review boards could evaluate impact assessments, approve vendor contracts, and handle student complaints together. This structure mirrors ethics committees already common within research institutions handling sensitive human data. Universities without existing ethics infrastructure could adapt those established processes for proctoring oversight specifically. Regular board meetings would also create institutional memory, improving decisions as proctoring technology continues evolving. Students could gain a clear, single point of contact for privacy-related concerns through this structure. This recommendation strengthens institutional accountability beyond what individual data protection officers can achieve alone. Interdisciplinary oversight produces more balanced, defensible decisions than isolated departmental review processes (Smith et al., 2011).

The implementation should proceed gradually through pilot programs before nationwide mandatory rollout begins. Foundational privacy scholarship reminds regulators that meaningful privacy protection develops through iterative practice, not sudden imposition. Selected universities could pilot the amendment's requirements for one academic year before broader adoption. Pilot results would reveal practical difficulties invisible during purely theoretical legislative drafting discussions. Regulators could then refine specific requirements based on genuine institutional experience rather than assumption alone. This phased approach also gives universities realistic time to build necessary internal capacity properly. Nationwide mandatory compliance could follow once pilot lessons inform a refined, tested final requirement. Clear communication throughout this process would help universities understand expectations and available support resources. Monitoring and periodic review should continue even after full nationwide implementation formally begins. A gradual, evi-

dence-based rollout gives this reform the strongest possible chance of lasting success (Westin, 2019).

E. Implications of the Proposed Amendment to the Law on Personal Data (No. ZRU-547)

The proposed amendment carries a direct implication for Uzbekistan's broader information security governance. Strengthening biometric data rules inside education technology reflects a wider national security priority already emerging elsewhere. Recent scholarship links robust legal mechanisms directly to effective information security within any digital economy. Proctoring surveillance generates sensitive data streams that, if mishandled, create genuine security vulnerabilities nationwide. Treating this data with the same seriousness as financial or governmental information matters considerably. The amendment signals that education technology deserves equal security attention alongside more traditional regulated sectors. This shift could encourage other sensitive technology sectors to expect similarly targeted legal treatment eventually. Strengthening one sector's information security framework often creates useful precedent for broader regulatory development. Regulators elsewhere may look toward this specific reform when addressing their own emerging technology gaps. This implication extends well beyond higher education into Uzbekistan's wider digital security architecture (Akhmedova & Khamidov, 2023).

A second important implication concerns artificial intelligence governance within Uzbekistan's evolving legal framework generally. Automated proctoring relies heavily on artificial intelligence to detect and flag student behavior. Recent research identifies significant regulatory gaps specifically around artificial intelligence and personal data processing nationally. The proposed amendment addresses one concrete instance of this broader, still-developing regulatory challenge directly. Requiring impact assessments before deployment offers a practical template applicable to other algorithmic systems too. Lawmakers drafting future artificial intelligence regulation could study this proctoring-specific amendment as a working model. Its consent and assessment requirements translate abstract artificial intelligence governance principles into concrete, testable institutional obligations. This makes the amendment relevant beyond education, informing Uzbekistan's parliament as it considers broader artificial intelligence legislation. Early, sector-specific experience often shapes more effective general rules developed later through legislative refinement. The amendment therefore contributes practical lessons toward Uzbekistan's still-forming artificial intelligence governance framework (Rakhimov & Turaev, 2026).

The amendment also implies a strengthened, more clearly defined role for the authorized state body. Research on enforcement highlights how much practical protection depends on the regulator's specific defined powers. Currently, education technology sits somewhat outside the authorized body's most detailed operational attention nationally. The amendment would require this authority to review, approve, or monitor proctoring impact assessments directly. This expands the regulator's practical mandate into a previously underdeveloped area of institutional oversight. Clearer authority over education technology

strengthens the regulator's institutional standing and recognized expertise significantly. Universities would gain a defined point of contact for questions about proctoring compliance specifically. This clarity benefits both the regulator, seeking efficient oversight, and universities, seeking predictable compliance guidance. Strengthening enforcement authority in one sector often improves institutional capacity for handling other sectors too. This implication positions the regulator for a more active, visible role in future technology governance (Saidova, 2023).

Another significant implication concerns how universities understand their own obligations as personal data operators specifically. Recent scholarship clarifies operator obligations and corresponding liability whenever personal data rules are violated directly. Universities have not always recognized themselves clearly as operators bearing these specific legal responsibilities. The amendment makes this operator status explicit within the context of automated proctoring technology specifically. Universities failing to conduct required impact assessments would face clearer, more direct legal consequences. This clarity discourages careless adoption of proctoring technology without proper prior institutional consideration. It also gives students a clearer legal basis for holding universities accountable when violations occur. Defined liability tends to produce more careful, deliberate institutional decision-making around sensitive data handling generally. Universities across Uzbekistan would need to review their existing proctoring arrangements against this clearer obligation. This implication encourages more responsible institutional behavior throughout the higher education sector (Yuldasheva, 2025).

The amendment also carries meaningful implications for constitutional human rights protection within Uzbekistan's legal system. Recent constitutional revisions explicitly protect individual freedoms against arbitrary institutional or state action nationwide. Extending impact assessment and consent requirements into proctoring directly supports these broader constitutional commitments. Students gain concrete institutional protection matching the spirit of these recently strengthened constitutional guarantees. This alignment demonstrates that constitutional principles can translate into specific, sector-relevant statutory protection meaningfully. Scholars studying constitutional reform often note gaps between broad guarantees and everyday institutional practice specifically. The proposed amendment helps close exactly this kind of gap within one clearly defined educational context. Other sectors facing similar surveillance technology could draw on this example when developing their own protections. Constitutional rights become more meaningful when supported by concrete, sector-specific legal mechanisms like this one. This implication strengthens the practical, lived experience of constitutional privacy protection for ordinary students (Habibjonov, 2024).

The amendment additionally signals a broader pattern of sector-specific consumer and user protection across Uzbekistan's digital economy. Recent scholarship on digital consumer protection highlights similar legal mechanisms developed for online shopping and e-commerce. Both contexts share a common structure: technology collecting personal data from individuals with limited practical alternatives. Students facing mandatory proctoring

resemble consumers facing mandatory data collection during ordinary digital transactions online. Applying similar protective logic to education strengthens regulatory consistency across different digital sectors nationally. This consistency helps citizens develop reasonable, stable expectations about their rights across various digital services. It also simplifies future legal drafting, since regulators can adapt proven models from one sector elsewhere. The proposed amendment therefore fits within a wider, coherent movement toward sector-specific digital protection nationwide. This pattern suggests Uzbekistan's regulatory approach is maturing beyond broad general rules alone. The implication extends this maturing pattern specifically into the higher education sector directly (Juraeva, 2024).

Finally, the amendment implies deeper integration between personal data law and Uzbekistan's wider digital legal ecosystem generally. Recent legal scholarship on electronic commerce highlights how data protection increasingly threads through nearly every digital-economy sector. Personal data rules no longer function as an isolated legal topic separate from everyday digital activity. Education technology, e-commerce, and financial services increasingly share overlapping personal data protection concerns and mechanisms. The proposed amendment reinforces this interconnected legal landscape by extending consistent principles into education specifically. Future legal reforms across other sectors will likely reference similar impact assessment and consent structures. This creates a more unified, predictable legal environment for both citizens and digital service providers generally. Universities, businesses, and regulators all benefit from this growing coherence across previously separate legal domains. The amendment therefore represents more than isolated education reform; it strengthens Uzbekistan's broader digital legal architecture. This final implication situates the proposed reform within Uzbekistan's larger, ongoing digital legal transformation (Ruzinazarov, 2026).

V. CONCLUSION

Automated exam surveillance forces universities to choose between academic control and student privacy. This study examined that tension within Uzbekistan's higher education system specifically. Cameras, microphones, and behavior-tracking software now watch students inside their own homes. Institutions adopted these tools quickly, without matching legal or ethical safeguards. This gap matters because education increasingly depends on digital platforms worldwide. Students across Central Asia now sit exams under constant algorithmic observation regularly. Uzbekistan's rapid digital transformation makes this question especially timely and relevant today. The country continues modernizing its data protection framework amid expanding online education. Universities elsewhere face similar pressures as remote assessment becomes permanent practice. This research situates a local legal problem within a much larger global pattern. Balancing integrity and privacy is not simply an Uzbek concern alone. It reflects a challenge facing every education system adopting surveillance-based assessment tools today.

Three connected findings anchor this study's central argument throughout the analysis presented earlier. Biometric data collected during proctoring qualifies as especially sensitive,

requiring stronger legal treatment. Algorithmic decision-making within these systems remains opaque, leaving students unable to challenge flagged results. Uzbekistan's Law on Personal Data, though comprehensive generally, contains no rules addressing this specific risk. These three findings reinforce one another closely rather than standing as separate, isolated observations. Weak transparency deepens the harm caused by unprotected biometric collection during examinations. Regulatory silence then allows both problems to continue without institutional correction or oversight. Together, they demonstrate why general privacy law cannot adequately govern specialized surveillance technology. This connected pattern directly supports the proposed amendment requiring impact assessment and specific consent. The amendment addresses each identified weakness through one coordinated legislative mechanism. Its design reflects the interconnected nature of the underlying problems it directly targets.

These findings carry weight beyond individual universities or any single academic term. Strengthening biometric protection in education could inform Uzbekistan's wider artificial intelligence and data governance efforts. Universities gain a practical framework for evaluating any future surveillance technology responsibly. Regulators gain a tested model for extending similar protections into other digital sectors. Students gain concrete assurance that assessment tools respect their fundamental privacy rights. Policymakers reviewing Uzbekistan's ongoing legislative reforms could adopt this amendment as immediate next steps. Future research should examine how students actually experience proctoring once new safeguards take effect. Comparative studies across neighboring Central Asian countries would also strengthen regional policy coordination meaningfully. Questions about long-term psychological effects of exam surveillance remain largely unanswered and deserve attention. This study offers one concrete legislative proposal within a much larger, ongoing conversation. Balancing academic control with student privacy remains an urgent, unfinished task for policymakers ahead.

VI. BIBLIOGRAPHY

Abdullaeva, D. K., et al. (2023). Cybersecurity issues in Uzbekistan. In *Soft Law on Cybersecurity and Data Governance* (pp. 167–189). https://doi.org/10.5040/9781509983759.ch-009

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2022). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 32*(1), 10–29.

Akhmedova, M., & Khamidov, A. (2023). Legal mechanisms for ensuring information security in the digital economy of Uzbekistan. *Journal of Law and Digital Society, 2*(1), 45–62. https://doi.org/10.5281/zenodo.10334521

Akmal, S. (2025). Legal evolution of human rights protection in Uzbekistan amid digital transformation. Cyberleninka. https://doi.org/10.5281/zenodo.17528864

AllahRakha, N. (2024a). Legal procedure for investigation under the Criminal Code of Uzbekistan. *International Journal of Law and Policy, 2*(3), 16–37. https://doi.org/10.59022/ijlp.160

AllahRakha, N. (2024b). Practices of the advertisement legislation of the Republic of Uzbekistan. *Yurisprudensiya, 4*(1), 73–89. https://doi.org/10.51788/tsul.jurisprudence.4.1./JGLN3011

Amaniyazova, S. B. (2023). Stages of formation of legal and conceptual foundations of digitalization processes in the Republic of Uzbekistan. *Journal of Foreign Legislation and Comparative Law, 18*(5).

Anorboev, A. (2026). *Personal data law: Personal data protection in the new era* [Monograph]. Dimal Publishing House. https://doi.org/10.5281/zenodo.21374052

Archer, E. (2023). Technology-driven proctoring: Validity, social justice and ethics in higher education. *Perspectives in Education, 41*(1), 119–136. https://doi.org/10.38140/pie.v41i1.6666

Baxodirov, A. (2026). Constitutional safeguards for digital rights and privacy in Uzbekistan. *Journal of Digital Law and Innovation*. https://doi.org/10.59022/ujldp.172

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario, Canada.

Coghlan, S., Miller, T., & Paterson, J. (2021). Good proctor or "Big Brother"? Ethics of online exam supervision technologies. *Philosophy & Technology, 34*(4), 1581–1606. https://doi.org/10.1007/s13347-021-00476-1

Eshdavlatova, Z. N. (2022). Raqamli texnologiyalar davrida shaxsiy ma'lumotlarni muhofaza qilish [Personal data protection in the era of digital technologies]. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences, 2*(4), 449–453.

Greenleaf, G. (2025). Data privacy laws in Central Asia: Between ex-SSR and 'Belt & Road'. *International Data Privacy Law, 15*(1), 67–89.

Habibjonov, I. D. (2024). Guarantees of individual freedoms in the newly revised constitution of the Republic of Uzbekistan. *Oriens, 4*(8), 111–116.

Han, S., Nikou, S., & Ayele, W. Y. (2024). Digital proctoring in higher education: A systematic literature review. *International Journal of Educational Management, 38*(1), 265–285. https://doi.org/10.1108/IJEM-12-2022-0522

Heinrich, E. (2025). A systematic-narrative review of online proctoring systems and a case for open standards. *Open Praxis, 17*(3), 485–500. https://doi.org/10.55982/openpraxis.17.3.836

Juraeva, N. (2024). Consumer in the digital space: Legal mechanisms for protection when shopping online. *Society and Innovations*.

Khalil, M., Prinsloo, P., & Slade, S. (2022). In the nexus of integrity and surveillance: Proctoring (re)considered. *Journal of Computer Assisted Learning, 38*(6), 1589–1602. https://doi.org/10.1111/jcal.12713

Khidirova, D. (2026). Institutional mechanisms for legal compliance and the protection of entrepreneurship in the Republic of Uzbekistan. *Society and Innovations*. https://doi.org/10.47689/2181-1415-vol7-iss4/S-pp724-735

Khodzhanova, M. A. (2024). Sravnenie normativno-pravovogo obespecheniya zashiti personal'nikh dannikh v zarubezhnikh stranakh i v Uzbekistan [Comparison of legal support for personal data protection in foreign countries and in Uzbekistan]. *Oriens.uz*, 463–472.

Koryog'diyev, B. U. (2023). O'zbekistonda shaxsiy hayot daxlsizligiga bo'lgan huquqlarni fuqarolik huquqiy tartibga solish [Civil-legal regulation of privacy rights in Uzbekistan]. *Oriens.uz*.

Makhkamova, M. (2025). Shaxsiy ma'lumotlarni boshqarishning qiyosiy tahlili: O'zbekiston va xalqaro standartlar [Comparative analysis of personal data management: Uzbekistan and international standards]. *Society and Innovations*.

Malhotra, M. (2026). Ensuring academic integrity through automated online exam proctoring: A decade-long systematic review. *Discover Education, 5*(1), 1–31. https://doi.org/10.1007/s44217-026-01224-3

Maphalala, M. C., & Nkosi, N. (2025). Proctoring online assessments: Enhancing security and academic integrity in open distance eLearning. *Open Praxis, 17*(4), 501–518. https://doi.org/10.55982/openpraxis.17.4.911

Marano, E., Newton, P. M., Birch, Z., Croombs, M., Gilbert, C., & Draper, M. J. (2024). What is the student experience of remote proctoring? A pragmatic scoping review. *Higher Education Quarterly, 78*(3), 1031–1047. https://doi.org/10.1111/hequ.12506

Muhammadjonova, M. (2025). The crucial role of English in advancing information security in Uzbekistan. *Shokh Journal*. https://doi.org/10.5281/zenodo.15666116

Mutimukwe, C. (2026). Privacy in online proctoring systems in higher education: Stakeholders' perceptions, awareness, and responsibility. *Journal of Computing in Higher Education*. Advance online publication. https://doi.org/10.1007/s12528-025-09461-5

Mutimukwe, C., Han, S., Viberg, O., & Cerratto-Pargman, T. (2023). Privacy as contextual integrity in online proctoring systems in higher education: A scoping review. *Proceedings of the 56th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2023.010

Nyssankuatova, D., Kassymova, L., Mamyrbekov, N., Mukazhanova, A., & Zholdybaeva, S. (2026). Information security management: Cybersecurity policy and digital data protection in Central Asia. *Journal of Information Policy, 16*, 5–25. https://doi.org/10.5325/jinfopoli.16.2026.0005

Ollaberganov, J. (2026). Media makonida shaxsiy daxlsizlik huquqi: Ijtimoiy tarmoqlarda shaxsga doir ma'lumotlarni himoya qilishning dolzarb masalalari [The right to personal inviolability in media space: Urgent issues of protecting personal data on social networks]. *Tamaddun Nuri Jurnali, 6*(81), 51–54. https://doi.org/10.69691/x7f34668

Otaboyev, N. (2026). Protecting personal data in the age of dominant tech giants: An empirical analysis of Uzbekistan. *Startups and Innovation Ecosystem, 1*(1), 1–8. https://doi.org/10.5281/zenodo.20796300

Rakha, A. (2023). Cyber law: Safeguarding digital spaces and personal data in Uzbekistan. *International Journal of Law and Policy*. https://doi.org/10.59022/ijlp.27

Rakhimov, S., & Turaev, A. (2026). Artificial intelligence and personal data processing: Regulatory gaps in Uzbekistan's legal framework. *AI & Society: Law and Ethics, 11*(1), 15–30.

Ruzinazarov, S. (2026). *Legal issues of electronic commerce in the new Uzbekistan* (Vol. 1). LAP Lambert Academic Publishing.

Sagymbaev, A. (2026). International information security in the era of digitalization: The case of Uzbekistan. *Premier Science*. https://doi.org/10.5281/zenodo.16789068

Saidova, D. (2023). The role of the authorized state body in enforcing the Law "On Personal Data" in Uzbekistan. *Uzbekistan Journal of Public Administration, 7*(4), 201–215. https://doi.org/10.5281/zenodo.10887432

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Vapayev, K. M. (2023). Unutilishga bo'lgan huquqning ayrim masalalari [Some issues of the right to be forgotten]. 336–351.

Westin, A. F. (2019). *Privacy and freedom* (Reissued ed.). Ig Publishing.

Xushvaqtova, E. (2024). Shaxsiy ma'lumotlar: Tushunchalar, turlar va subyektlar [Personal data: Concepts, types, and subjects]. *Journal of Science-Innovative Research in Uzbekistan*. https://doi.org/10.5281/zenodo.11215553

Yuldashev, J. I. (2024). Problems of legal regulation of personal data protection in the Republic of Uzbekistan. Zenodo. https://doi.org/10.5281/zenodo.14061162

Yuldasheva, G. (2025). Shaxsiy ma'lumotlar operatorlarining majburiyatlari va ularning buzilishi uchun javobgarlik [Obligations of personal data operators and liability for their violation in Uzbekistan]. *Huquqiy Axborot Jurnali, 12*(1), 55–68. https://doi.org/10.5281/zenodo.14992011

Yusupova, N., & Ergashev, B. (2024). Digital rights enforcement in transitional economies: A case study of Uzbekistan's 2019 Personal Data Law. *Central Asian Law Review, 3*(1), 45–67.