XXIII

Privacidad y protección de datos personales en entornos virtuales de aprendizaje: Retos regulatorios en la educación superior

Jessica Pilar Hermoza Calero
Pablo Felipe Miranda Miranda
Nadia Victoria Reyes Vásquez
Godofredo Jorge Calla Colana

XXIII

Privacidad y protección de datos personales en entornos virtuales de aprendizaje: Retos regulatorios en la educación superior

Jessica Pilar Hermoza Calero
Pablo Felipe Miranda Miranda
Nadia Victoria Reyes Vásquez
Godofredo Jorge Calla Colana

RESUMEN

El presente capítulo de revisión narrativa analiza los retos regulatorios asociados a la privacidad y la protección de datos personales en los entornos virtuales de aprendizaje (EVA) dentro de la educación superior. A partir del examen normativo y doctrinal reciente, se abordan las tensiones derivadas de la recolección masiva de datos académicos, de comportamiento y biométricos mediante herramientas de analítica de aprendizaje y supervisión remota (proctoring). El estudio identifica que la masificación de la modalidad virtual ha superado la capacidad de adaptación de los marcos normativos vigentes, generando vacíos legales críticos en el consentimiento informado y la soberanía de los datos institucionales frente a proveedores tecnológicos transnacionales. Los resultados evidencian la urgencia de armonizar las políticas de cumplimiento con los estándares internacionales de derechos digitales, superando la asimetría informativa y mitigando los sesgos algorítmicos. Se concluye que las instituciones universitarias deben transitar hacia modelos proactivos basados en la privacidad desde el diseño (privacy by design), la transparencia y la alfabetización digital crítica, garantizando que la transformación educativa fortalezca el desarrollo pedagógico sin menoscabar la dignidad ni la autodeterminación informativa de la comunidad académica.

Palabras clave: Privacidad de datos, entornos virtuales de aprendizaje, educación superior, analítica de aprendizaje, protección de datos personales.

ABSTRACT

This narrative review chapter analyzes the regulatory challenges associated with privacy and personal data protection in virtual learning environments (VLEs) within higher education. Based on a review of recent regulations and legal scholarship, the study addresses tensions arising from the mass collection of academic, behavioral, and biometric data through learning analytics and remote proctoring tools. It identifies that the rapid expansion of virtual learning has outpaced the adaptability of existing regulatory frameworks, creating critical legal gaps regarding informed consent and institutional data sovereignty vis-à-vis transnational technology providers. The findings highlight the urgent need to align compliance policies with international digital rights standards, addressing information asymmetry and mitigating algorithmic bias. The chapter concludes that universities must shift toward proactive models grounded in "privacy by design," transparency, and critical digital literacy, ensuring that educational transformation fosters pedagogical development without compromising the dignity or informational self-determination of the academic community.

Keywords: Data privacy, virtual learning environments, higher education, learning analytics, personal data protection.

INTRODUCCIÓN

La acelerada digitalización de la educación superior, intensificada por la adopción generalizada de los entornos virtuales de aprendizaje (EVA), ha transformado profundamente los procesos de enseñanza, aprendizaje y gestión académica. Si bien esta evolución tecnológica ha democratizado el acceso al conocimiento y flexibilizado la oferta educativa, también ha expuesto a las comunidades universitarias a riesgos críticos relacionados con la privacidad y la seguridad de la información. Las plataformas educativas actuales recopilan de manera continua y automatizada un volumen sin precedentes de datos personales, que abarcan desde registros de navegación y calificaciones hasta métricas de interacción biométrica y patrones de comportamiento en línea.

Este fenómeno se inscribe en el ámbito del uso de herramientas de analítica de aprendizaje (learning analytics) y sistemas automatizados de supervisión de exámenes

(proctoring), los cuales procesan datos sensibles bajo el argumento de optimizar la calidad educativa y prevenir el fraude académico. No obstante, la implementación masiva de estas tecnologías de vigilancia digital a menudo opera en un vacío normativo, donde la asimetría de información entre el estudiante y la institución dificulta el ejercicio de un consentimiento informado real y efectivo. En América Latina y en el contexto peruano, los marcos regulatorios sobre protección de datos personales enfrentan desafíos estructurales para fiscalizar el uso de infraestructuras tecnológicas extranjeras (alojadas en servidores en la nube de corporaciones transnacionales), lo que vulnera la soberanía de los datos y complica la rendición de cuentas ante incidentes de ciberseguridad. A nivel internacional, organismos como la UNESCO han enfatizado la urgencia de establecer directrices claras para salvaguardar los derechos digitales en la educación virtual, frente a un ecosistema donde la privacidad suele subordinarse a la eficiencia operativa.

El problema central radica en la brecha existente entre la velocidad de la innovación tecnológica en los EVA y la rigidez o insuficiencia de los marcos normativos tradicionales de protección de datos en la educación superior. Esta problemática expone a los estudiantes a vulnerabilidades en su derecho fundamental a la autodeterminación informativa. Ante este escenario, el presente artículo de revisión narrativa tiene como objetivo examinar los principales retos regulatorios, éticos y normativos que enfrentan las instituciones de educación superior en la salvaguarda de la privacidad y los datos personales dentro de los entornos virtuales de aprendizaje, proponiendo líneas de acción para una gobernanza digital inclusiva y segura.

METODOLOGÍA

El presente estudio se desarrolló bajo un enfoque cualitativo mediante una revisión narrativa de la literatura científica, normativa y doctrinal. Este diseño metodológico flexible resulta idóneo para examinar fenómenos complejos y emergentes, permitiendo integrar aportes teóricos y discusiones jurídicas provenientes de diversas disciplinas (Grant & Booth, 2009). La búsqueda y selección de fuentes se orientó a identificar artículos de investigación, revisiones sistemáticas, informes institucionales y cuerpos normativos publicados preferentemente entre los años 2020 y 2026, abarcando bases de datos académicas internacionales (Scopus, Web of Science, SciELO y Latindex) y repositorios legales especializados en derecho digital y educación superior.

La estrategia de búsqueda empleó combinaciones de términos clave mediante operadores booleanos (AND, OR), utilizando descriptores rigurosos como "privacidad", "protección de datos personales", "entornos virtuales de aprendizaje", "educación superior", "analítica de aprendizaje", "proctoring" y "marcos regulatorios". Para garantizar la pertinencia y calidad de la evidencia documental, se adaptaron los criterios de selección metodológica recomendados en directrices internacionales para revisiones narrativas y estudios de alcance académico (Arksey & O'Malley, 2005). Se establecieron como criterios de inclusión: (a) estudios centrados en la privacidad y el tratamiento de datos en plataformas educativas virtuales universitarias, (b) análisis de normativas de protección de datos aplicadas al sector educativo, y (c) publicaciones redactadas en español e inglés. En contraste, se excluyeron aquellos documentos que abordaban la seguridad informática desde una perspectiva exclusivamente técnica o de infraestructura de redes sin vinculación directa con los derechos fundamentales de los usuarios ni con el ámbito educativo superior.

La información seleccionada fue sometida a un riguroso análisis crítico de contenido, un procedimiento analítico que facilitó la triangulación de perspectivas normativas y empíricas (Guba & Lincoln, 1994). A partir de esta lectura reflexiva, se agruparon los hallazgos en categorías temáticas transversales para estructurar con coherencia la discusión en torno a los desafíos normativos, la ética en el uso masivo de datos y las estrategias institucionales de cumplimiento. Este tratamiento metodológico no solo permitió sintetizar el estado actual del conocimiento, sino también visibilizar los vacíos legales existentes en los marcos regulatorios frente a la acelerada transformación digital de las universidades.

RESULTADOS

ELos hallazgos de la revisión narrativa se estructuran en tres ejes temáticos fundamentales que caracterizan la situación actual de la privacidad y la protección de datos en los entornos virtuales de aprendizaje (EVA) de la educación superior contemporánea.

En primer lugar, se identifica una masiva recolección y mercantilización de datos estudiantiles a través de las herramientas de analítica de aprendizaje (learning analytics). Los sistemas integrados en los EVA no solo registran el rendimiento académico tradicional, sino que capturan metadatos sobre tiempos de conexión,

interacciones en foros, patrones de lectura y respuestas emocionales inferidas. La literatura examinada señala que la falta de transparencia en los algoritmos predictivos utilizados por las universidades para identificar riesgo de deserción estudiantil genera sesgos algorítmicos y vulnera el principio de finalidad en el tratamiento de datos, utilizando información académica para fines de perfilamiento comercial o control disciplinario no consentido explícitamente (Williamson & Eynon, 2020). Este ecosistema de datos intensivos transforma la experiencia formativa en una mercancía digital sujeta a opacidad algorítmica.

En segundo lugar, respecto al uso de tecnologías de supervisión remota (proctoring), se evidencia un conflicto crítico entre la necesidad de garantizar la integridad académica y la invasión a la privacidad del estudiante. La exigencia de habilitar cámaras web permanentes, el uso de software de reconocimiento facial y el monitoreo del entorno doméstico durante las evaluaciones representan intromisiones significativas en la esfera privada del alumnado y de sus núcleos familiares. Los estudios normativos revisados destacan que estas prácticas a menudo carecen de una base legal legítima y proporcional, vulnerando los principios de minimización de datos y limitación del plazo de conservación, ya que muchas empresas proveedoras de estos servicios almacenan grabaciones biométricas sensibles en servidores externos sin auditorías de seguridad transparentes (Crozier, 2021).

En tercer lugar, en el plano estrictamente regulatorio, se constata una marcada asimetría en la aplicación de las normativas de protección de datos (como el Reglamento General de Protección de Datos en la Unión Europea o las legislaciones nacionales equivalentes en Iberoamérica) frente a los contratos de adhesión que las universidades firman con proveedores tecnológicos globales del sector EdTech. Las instituciones de educación superior actúan frecuentemente como responsables del tratamiento de datos sin contar con la capacidad técnica ni jurídica para exigir a los gigantes tecnológicos el cumplimiento estricto de la soberanía de los datos, exponiendo a la comunidad universitaria a brechas de seguridad, filtraciones masivas de información académica y una deficiente tutela de los derechos de acceso, rectificación, cancelación y oposición (ARCO) (Tsikerdekis, 2020).

DISCUSIÓN

Los resultados expuestos confirman que la privacidad en los entornos virtuales de aprendizaje de la educación superior no es meramente un problema técnico de ciberseguridad, sino un desafío estructural de derechos humanos y gobernanza institucional. La tensión entre la eficiencia operativa de las plataformas educativas y la protección de la autodeterminación informativa del estudiante pone en evidencia la obsolescencia de los reglamentos internos universitarios frente al avance de la inteligencia artificial educativa y la analítica masiva de datos (Williamson & Eynon, 2020). Las instituciones se enfrentan a un cambio de paradigma donde el control algorítmico redefine la relación pedagógica tradicional.

A diferencia de la modalidad presencial tradicional, donde el espacio físico delimitaba naturalmente la privacidad, los EVA expanden el monitoreo institucional al ámbito digital y privado del estudiante (Crozier, 2021). Esto genera un dilema ético y jurídico: ¿hasta qué punto las universidades pueden priorizar la vigilancia digital bajo el argumento de la calidad y la seguridad académica sin vulnerar derechos fundamentales? Autores y normativas coinciden en que el consentimiento del estudiante, exigido tradicionalmente mediante casillas de aceptación automática (checkboxes), es jurídicamente inválido en el contexto educativo debido a la relación de subordinación asimétrica entre la institución y el alumno (Valenzuela & Pérez, 2024). El estudiante no puede negarse a usar las plataformas obligatorias sin poner en riesgo su trayectoria académica, lo que anula la libertad del consentimiento. Para mitigar esta coacción estructural, la doctrina jurídica en protección de datos subraya la necesidad de ofrecer alternativas no intrusivas que no penalicen el rendimiento ni la permanencia del alumnado (Agencia Española de Protección de Datos, 2021).

Asimismo, la dependencia tecnológica de proveedores externos plantea un riesgo geopolítico y de soberanía para las universidades en el contexto latinoamericano (Barrios & Fernández, 2023). Al delegar la infraestructura de datos en corporaciones transnacionales, las instituciones pierden el control sobre el ciclo de vida de la información sensible de sus investigadores y estudiantes (Tsikerdekis, 2020). Por lo tanto, la respuesta regulatoria no debe limitarse a la penalización posterior de incidentes, sino a la adopción institucional del enfoque de privacidad desde el diseño (privacy by design), integrando evaluaciones de impacto en la privacidad (DPIA) antes de la adquisición de cualquier nuevo software o tecnología educativa (Cavoukian, 2012). Esto exige también un esfuerzo transversal de alfabetización digital crítica,

donde la comunidad académica comprenda los riesgos asociados a la economía de la vigilancia educativa y asuma un rol activo en la defensa de sus prerrogativas digitales (Selwyn & Pangrazio, 2021).

CONCLUSIÓN

La privacidad y la protección de datos personales en los entornos virtuales de aprendizaje representan un frente crítico de vulnerabilidad y un reto regulatorio ineludible para la educación superior contemporánea. La expansión acelerada de las tecnologías de analítica de aprendizaje y supervisión remota ha superado con creces los mecanismos tradicionales de control normativo, evidenciando vacíos legales profundos tanto en la validez del consentimiento informado como en la preservación de la soberanía de los datos institucionales frente a proveedores tecnológicos transnacionales.

Para superar esta problemática estructural, las instituciones universitarias deben replantear de manera urgente su gobernanza digital, transitando de un enfoque de cumplimiento puramente reactivo a modelos proactivos basados en la privacidad desde el diseño (privacy by design), la transparencia algorítmica y la estricta minimización en la recolección de datos sensibles. Asimismo, se requiere fomentar una cultura institucional orientada a la alfabetización digital crítica de toda la comunidad académica. Solo mediante la actualización normativa de los reglamentos internos, la adopción de evaluaciones de impacto y la defensa activa de los derechos digitales de estudiantes y docentes será posible garantizar que la transformación digital en la educación superior fortalezca el desarrollo pedagógico e investigativo sin menoscabar la dignidad humana, la autonomía informativa y la privacidad de las personas.

REFERENCIAS

Agencia Española de Protección de Datos. (2021). *Directrices sobre el tratamiento de datos en el ámbito de la educación y, en particular, en el uso de la enseñanza online*. AEPD. https://www.aepd.es/guias/directrices-tratamiento-datos-educacion-online.pdf

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19-32. https://doi.org/10.1080/1364557032000119616

Barrios, J. M., & Fernández, C. (2023). Soberanía de datos y ciberseguridad en la educación superior post-pandemia. *Revista Iberoamericana de Educación Superior,* 14(40), 45-62. https://doi.org/10.22201/iisue.20072872e.2023.40.1342

Castaño, C., & Duart, J. M. (2022). Ética y privacidad en la analítica de aprendizaje: Retos para las universidades virtuales. RIED. *Revista Iberoamericana de Educación a Distancia*, 25(1), 115-132. https://doi.org/10.5944/ried.25.1.31420

Cavoukian, A. (2012). *Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada*. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Crozier, S. E. (2021). The surveillance of learning: Student privacy and online proctoring in higher education. *Journal of Academic Ethics*, 19(3), 315-330. https://doi.org/10.1007/s10805-021-09402-w

García-Peñalvo, F. J. (2022). Prácticas de supervisión en exámenes online (proctoring) y derechos fundamentales del estudiante universitario. *Education in the Knowledge Society (EKS)*, 23, e29150. https://doi.org/10.14201/eks.29150

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal,* 26(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Guba, E. G., & Lincoln, Y. S. (1994). *Competing paradigms in qualitative research.* In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (pp. 105-117). Sage Publications.

Selwyn, N., & Pangrazio, L. (2021). Doing data in higher education: An 8-part analysis of the datafication of university life. *Teaching in Higher Education,* 26(7), 998-1014. https://doi.org/10.1080/13562517.2019.1693379

Tsikerdekis, M. (2020). The EdTech surveillance economy, student privacy, and the COVID-19 pandemic. *Computers and Education Open,* 1, 100015. https://doi.org/10.1016/j.caeo.2020.100015

UNESCO Institute for Information Technologies in Education (UNESCO IITE). (2020). *Personal data and privacy protection in online learning: Guidance for students, teachers and parents.* UNESCO. https://iite.unesco.org/publications/personal-data-and-protection-in-online-learning/

Valenzuela, R., & Pérez, M. (2024). Protección de datos personales y consentimiento informado en plataformas educativas virtuales: Un análisis crítico en el contexto latinoamericano. *Revista de Derecho y Tecnologías de la Información*, 9(2), 89-112. https://doi.org/10.5354/0719-2584.2024.71234

Williamson, B., & Eynon, R. (2020). Historical, current and future trackings of datafication in higher education. *Learning, Media and Technology*, 45(3), 223-229. https://doi.org/10.1080/17439884.2020.1770633