

Capítulo 2

Protección de datos personales y educación digital: desafíos éticos en la comunidad universitaria durante la Cuarta Revolución Industrial

Lizeth Guadalupe Valenzuela Álvarez
ORCID: 0000-0003-4508-9304

Facultad de Economía y Relaciones Internacionales
Universidad Autónoma de Baja California

<https://doi.org/10.61728/AE20252373>



Introducción

En el contexto de la Cuarta Revolución Industrial (4RI) y la economía de los datos, la protección de datos personales se ha convertido en un elemento crucial para la privacidad y seguridad de los seres humanos. Este capítulo explora la importancia de la protección de datos y la educación digital, centrándose en la comunidad universitaria de la Facultad de Economía y Relaciones Internacionales (FEyRI) de la Universidad Autónoma de Baja California (UABC). La gestión adecuada de los datos personales y la conciencia sobre los derechos digitales son esenciales para el bienestar de los estudiantes en un entorno tecnológico cada vez más complejo, donde los modos convencionales de utilizar y vivir con la tecnología representan más y variados retos.

La recopilación, procesamiento y almacenamiento de grandes cantidades de datos personales por parte de instituciones y empresas ha planteado nuevos desafíos en términos de privacidad y seguridad. La economía de los datos, que se basa en el uso intensivo de la información personal, ha generado preocupaciones sobre la vigilancia y el control de la información. En este contexto, la educación digital juega un papel fundamental para empoderar a los estudiantes, proporcionándoles las herramientas y conocimientos necesarios para proteger sus datos personales y ejercer sus derechos digitales de manera efectiva. La falta de conocimiento y conciencia sobre los derechos de privacidad y protección de datos puede llevar a la explotación de la información personal, afectando la autonomía y la dignidad humana. Por lo tanto, es crucial que las instituciones educativas implementen programas y políticas que fomenten una cultura de protección de datos y ética digital entre los estudiantes, preparándolos para enfrentar los desafíos de la 4RI y asegurar una gestión responsable de la información personal.

Protección de datos personales

En una sociedad en constante cambio, donde el espacio privado se reduce significativamente, la privacidad y la intimidad asumen un papel crucial. Desde el panóptico de Foucault hasta el Gran Hermano Orwelliano, el derecho enfrenta múltiples desafíos y convergencias (Tenorio, 2019). Ramirez et al. (2017) señalan que derecho a la protección de datos personales, es un derecho fundamental autónomo del derecho a la vida privada, ha evolucionado de manera asimétrica en diferentes sistemas de derechos humanos, influenciado por la evolución tecnológica, la digitalización de las relaciones humanas y la transición de una economía tradicional a una digital.

El derecho a la protección de datos personales busca salvaguardar la privacidad y el control sobre la información personal. Los instrumentos de protección responden a ciertos fenómenos originados desde la opacidad de las regulaciones, casos que en breve se señalarán. Es crucial que tanto individuos como organizaciones comprendan sus responsabilidades en la gestión de dicha información para prevenir riesgos y garantizar los derechos de los propietarios de esos datos (Serrano-Santoyo, 2018). La dinámica de los datos, las huellas digitales, los meta-ecosistemas hiperconectados, infraestructuras virtuales que registran cada acción, movimiento o voz que emite la *e-society*. García (2019) sostiene que este derecho debe ser respetado por todas las personas y organizaciones, enfatizando la importancia de la privacidad y el control de los datos para evitar vulnerabilidades. Destaca que el empoderamiento digital es clave en la protección de datos, ya que los usuarios deben ser conscientes de los riesgos y saber cómo proteger sus datos.

Las nuevas tecnologías plantean desafíos significativos a la privacidad de los datos personales, especialmente con el uso de la inteligencia artificial (IA) y los macrodatos. Martínez Devia (2019) argumenta que la recopilación y uso de datos personales en plataformas digitales genera importantes problemas de privacidad, sugiriendo actualizar las normas de protección de datos para otorgar a las personas mayor control sobre su información. Véliz (2021) menciona casos significativos de transgresión, como el escándalo de Cambridge Analytica y el caso de Malte

Spitz, destacando la necesidad de mayor transparencia y protección de la privacidad.

El caso de Malte Spitz, quien demandó a Deutsche Telekom para acceder a los datos de localización de su móvil, demostró la importancia de los datos personales y la necesidad de una mayor transparencia. Este caso influenció la legislación europea, incluida la aprobación del Reglamento General de Protección de Datos (RGPD) en 2016, estableciendo un marco legal más estricto para la protección de datos personales en Europa. Los ejemplos citados subrayan la necesidad de una regulación global y una gobernanza sólida sobre los datos personales.

Privacidad de los datos

La privacidad de datos es crucial en la era digital debido a los avances tecnológicos y la creciente necesidad empresarial, económica y del Estado de recopilar y utilizar información personal. Los datos personales, que identifican o hacen identificable a una persona, son esenciales para interactuar con otros y cumplir con las leyes. Sin embargo, la forma en que se recopilan y utilizan plantea preocupaciones éticas, económicas y sociales significativas. Es necesario abordar adecuadamente las cuestiones relacionadas con la privacidad de los datos personales (Tenorio, 2019; Cate, 2019).

Desde las políticas públicas, la privacidad se ha definido como lo opuesto a lo público, aunque esta definición no capta toda su complejidad. La privacidad también se entiende como una búsqueda de anonimato y clandestinidad. Los usuarios de internet están en desventaja en un mundo cada vez más público e interconectado. En este sentido, la privacidad es un derecho fundamental que protege la autonomía, independencia, poder y control sobre la información personal, tanto en el mundo físico como en el digital (Tenorio, 2019).

La privacidad, considerada un derecho humano desde hace mucho tiempo, implica el derecho a la vida privada, la protección de datos personales y el control sobre la información personal (Cate, 2019). La recopilación, procesamiento y uso de datos personales sin consentimiento puede ser invasiva y violar la privacidad de los usuarios, destacando la

necesidad de una regulación adecuada para proteger estos datos en línea (Prabhakara, 2021; Habermas, 1981).

La privacidad es esencial para la dignidad humana y no se limita a ocultar información. Es parte fundamental de la ética (Cortina, 2022). Habermas (1981) argumenta que la privacidad no debe sacrificarse en aras de la publicidad y la transparencia, destacando la necesidad de preservar la libertad individual.

José Luis Piñar Mañas planteó en 2010 la pregunta: ¿existe la privacidad? A lo largo de los años, los avances tecnológicos y las implicaciones éticas han desafiado el modelo económico de gestión de grandes cantidades de datos (Piñar Mañas, 2010). Tenorio (2021) y Zuboff (2020) argumentan que el capitalismo de la vigilancia utiliza la experiencia humana como materia prima gratuita, creando productos predictivos que prevén el comportamiento futuro.

La recopilación de datos personales es esencial para establecer la identidad de un individuo y permitir su interacción con otros. Estos datos también son fundamentales para el crecimiento económico y la mejora de bienes y servicios. Sin embargo, su uso debe ser ético, transparente y con el consentimiento explícito del individuo. La recopilación de datos debe limitarse a fines específicos (Mañas et al., 2010).

Los datos personales son esenciales para la identidad y la interacción social en la era digital. Su uso responsable y ético es fundamental para garantizar la privacidad y proteger los derechos de los individuos (Tenorio, 2019; Cate, 2019; Prabhakara, 2021)

Desafíos éticos

Este apartado subraya la importancia de que la tecnología beneficie a la sociedad en lugar de controlarla. En la actualidad, en medio de la revolución industrial, es crucial que los algoritmos se programen de manera ética, respetando el principio de “No-maleficencia”. Adela Cortina enfatiza que la tecnología no debe sobrepasarnos en conocimiento ni controlarnos; en su lugar, debe ayudarnos a comprender mejor nuestra conducta. A pesar de ser llamados “usuarios”, somos seres humanos con derechos y necesidades, y la tecnología debe servirnos, no al revés (Cortina, 2022).

El término “algoritmo” es familiar para muchos, pero a medida que estos se vuelven más complejos, nuestra comprensión sobre ellos disminuye. Estos algoritmos utilizan vastos conocimientos sobre cada usuario para motivar su actividad en diversas plataformas y productos inteligentes, como relojes y asistentes virtuales. La información contenida en los algoritmos incluye registros de nuestras actividades pasadas y predice futuras acciones, similar a la paradoja del gato de Schrödinger. Para nosotros, los algoritmos son una caja negra, y las consecuencias de su uso parecen inevitables. En síntesis, los algoritmos actúan como nuestro “anti-yo” al saber más sobre nosotros de lo que nosotros mismos sabemos, continuando y alimentando este aprendizaje indefinidamente que señala Turkle, (2011).

La privacidad de los datos personales es un desafío ético significativo en la sociedad digital actual, que está mutando hacia una sociedad transhumanista sin ser consultada (Cortina, 2022). Los avances deben orientarse hacia la sostenibilidad social y planetaria, respetando el principio de no-maleficencia, que implica no causar daño y prevenirlo. En cuanto a la posible sumisión a máquinas, es esencial respetar el principio de autonomía humana y evitar que las máquinas tomen decisiones éticas inherentes a los humanos. Esto se puede fortalecer con sistemas inteligentes donde el control y las decisiones significativas se mantengan en manos humanas, asegurando que la privacidad siga siendo un componente clave de la autonomía (Cortina, 2022).

La sociedad está delegando recuerdos a la tecnología, lo que puede llevar a una amnesia digital al depender excesivamente de la tecnología para recordar (Turkle, 2011). Las relaciones con la IA y los robots se están volviendo más complejas, creando conexiones emocionales con máquinas que pueden tener consecuencias tanto positivas como negativas (Turkle, 2011).

Hablar de una vida fuera del ecosistema tecnológico en 2022 sería como sugerir vivir en cavernas, según Cortina, haciendo referencia al mito de Platón. Las preocupaciones éticas sobre el uso de la tecnología y la generación de datos no son infundadas, ya que los gobiernos que no defienden la libertad de pensamiento pueden criminalizar creencias y opiniones mediante la tecnología (Tegmark, 2018).

Las tecnologías de la información presentan un desafío urgente respecto al derecho a la vida privada. Términos como *big data*, computación en la nube, *e-learning*, ciberacoso y ciberdelitos están reconfigurando el concepto de vida privada (Tenorio, 2021). Es crucial abordar estos desafíos y garantizar que la tecnología sirva a los humanos, respetando el principio de no-maleficencia, protegiendo la privacidad y promoviendo la explicabilidad y la responsabilidad (Cortina, 2022).

La ética en la era digital es compleja y ha generado brechas entre diversas aplicaciones tecnológicas. Según Zuboff (2020), el capitalismo de la vigilancia utiliza la experiencia humana como materia prima gratuita, creando productos predictivos que anticipan el comportamiento futuro. Esta lógica necesita ser repensada, y los tomadores de decisiones deben ser conscientes de su responsabilidad en la creación de opiniones sociales y la ética en la tecnología. Es esencial considerar las implicaciones éticas y prácticas responsables desde el diseño mismo de las tecnologías (Schneier, 2015).

Para cerrar este apartado, se debe de mencionar que la intersección entre la ética y la tecnología digital emergente es un terreno que requiere atención cuidadosa y acción decidida. La revolución tecnológica actual, caracterizada por la omnipresencia de algoritmos y sistemas inteligentes, plantea desafíos únicos que no pueden ser ignorados. A medida que las tecnologías digitales continúan evolucionando, es imperativo que su desarrollo y aplicación se guíen por principios éticos sólidos para evitar daños y promover el bienestar de la sociedad.

Los principios de no-maleficencia, autonomía, explicabilidad y responsabilidad deben estar en el centro de cualquier estrategia tecnológica. La no-maleficencia nos recuerda la obligación de no causar daño, y la autonomía refuerza la necesidad de respetar la capacidad de los individuos para tomar decisiones informadas sobre sus vidas y datos personales (Cortina, 2022). La explicabilidad es crucial para asegurar que los sistemas inteligentes sean comprensibles y transparentes, permitiendo a los usuarios entender cómo y por qué se toman ciertas decisiones. La responsabilidad implica que tanto los desarrolladores como los usuarios deben asumir las consecuencias de las acciones tecnológicas y trabajar activamente para mitigar cualquier impacto negativo. Es necesario abor-

dar la creciente desconexión entre nuestra identidad digital y nuestra vida real. Como señala Turkle (2011), las identidades en línea pueden convertirse en máscaras que ocultan nuestras verdaderas personalidades, creando una dicotomía entre lo virtual y lo real. Esta desconexión puede tener implicaciones significativas para la salud mental y el bienestar, destacando la necesidad de un enfoque equilibrado que considere tanto los beneficios como los riesgos de la tecnología.

La recopilación masiva de datos y su uso para fines comerciales o de vigilancia plantea serias preocupaciones sobre la privacidad y la seguridad. Los casos de Cambridge Analytica y Malte Spitz ilustran cómo los datos personales pueden ser explotados, subrayando la urgencia de una regulación robusta y la implementación de prácticas que protejan la privacidad (Véliz, 2021; Zuboff, 2020). Es fundamental que los marcos legales y las políticas públicas se mantengan al día con los avances tecnológicos para asegurar que los derechos de los individuos estén protegidos en todo momento. En este contexto, la educación y la concienciación juegan un papel vital. Los usuarios deben estar informados sobre los riesgos y beneficios de la tecnología para tomar decisiones informadas. La incorporación de la ética digital en los currículos educativos puede empoderar a la próxima generación para enfrentar los desafíos tecnológicos de manera responsable.

Finalmente, la ética en el diseño y uso de tecnologías emergentes no puede ser una consideración tardía. Desde la concepción hasta la implementación, la seguridad y la equidad deben ser prioridades integradas en todo el ciclo de vida de la tecnología (Schneier, 2015). Solo así podremos garantizar que las tecnologías digitales emergentes beneficien a la humanidad y no la perjudiquen.

Las implicaciones éticas de la tecnología son profundas y multifacéticas. Requieren una colaboración continua entre desarrolladores, reguladores y usuarios para asegurar que la tecnología se utilice de manera responsable y equitativa. La ética debe ser el faro que guíe nuestra navegación a través del complejo y dinámico paisaje digital, asegurando que las innovaciones tecnológicas contribuyan a un futuro mejor para todos.

Educación digital

Cada vez se observa una mayor conciencia y educación en el ámbito de los derechos digitales en los estudiantes. Muchas escuelas están tomando medidas para educar a los estudiantes sobre sus derechos y responsabilidades digitales, incluyendo temas como la privacidad en línea, el ciberacoso y la propiedad intelectual (ISTE, 2017). Las escuelas están implementando medidas de protección de datos más estrictos para garantizar que la información personal de los estudiantes se mantenga segura y privada (NCES, 2018). El Centro Nacional de Estadísticas Educativas (NCES) describe la responsabilidad de las escuelas en la protección de los datos de los estudiantes, sugiriendo que estas deben cumplir con las leyes federales y estatales relacionadas con la privacidad de los datos, como la Ley de Privacidad y Derechos Educativos de la Familia (FERPA).

El NCES hace varias recomendaciones en relación con la protección de los datos de los estudiantes en las escuelas, incluyendo la obtención del consentimiento de los padres antes de recopilar, usar o compartir datos de los estudiantes, y la necesidad de que las escuelas tengan políticas y procedimientos claros para la recopilación, uso y compartición de datos, comunicándolos a los padres, estudiantes y personal. El NCES sugiere que las escuelas implementen medidas de seguridad, como cifrado y protección con contraseña, para proteger los datos del acceso no autorizado. Es crucial que las escuelas también brinden capacitación sobre privacidad y seguridad de datos para garantizar que el personal y los educadores comprendan sus responsabilidades y sigan las mejores prácticas (NCES, 2018).

El Departamento de Educación de los Estados Unidos enfatiza la importancia de proteger la privacidad de los estudiantes, y recomienda que las escuelas solo recopilen y utilicen los datos de los estudiantes con fines educativos legítimos, y no los compartan con terceros sin el consentimiento de los padres o de los estudiantes en el caso de las universidades. También sugiere que las escuelas implementen prácticas seguras de administración de datos, como cifrado y protección con contraseña, y desarrollen planes de respuesta a la filtración de datos para mitigar cualquier posible brecha (US Department of Education, 2019).

La UNESCO (2015) propone repensar la educación para crear un bien común global, enfatizando que la educación es un derecho humano fundamental que debe promover la ciudadanía global, la paz y la sostenibilidad ambiental. Destaca el papel transformador de la tecnología en la educación, aumentando el acceso, mejorando la calidad y fomentando la innovación.

En México, la Estrategia Digital Nacional para la Educación busca promover el uso de la tecnología en la educación mientras protege la privacidad y seguridad de los datos de los estudiantes (SEP, 2020). La creación del Programa de Cultura Ciudadana Digital por parte de la Estrategia Digital Nacional promueve el comportamiento digital responsable entre estudiantes y docentes (Presidencia de la República, 2020). La modificación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2020 y el establecimiento del Consejo Nacional de Estrategia Digital en 2019 son pasos importantes para garantizar la seguridad y privacidad de los datos en el entorno digital educativo (Cámara de Diputados del H. Congreso de la Unión, 2020; Diario Oficial de la Federación, 2019). Estos avances reflejan un reconocimiento creciente de la importancia de los derechos digitales y la necesidad de protegerlos en el ámbito escolar en México.

A pesar de estos esfuerzos, se recomienda realizar ajustes estructurales y administrativos en las universidades para mejorar la construcción de capacidades y la difusión de conocimientos sobre privacidad y protección de datos. La Universidad Autónoma de Baja California (UABC) ha desarrollado iniciativas importantes para fomentar el conocimiento y la aplicación de la protección de datos y la privacidad. La Agencia de Transparencia y Acceso a la Información Pública (UTAIP) ha emitido avisos de privacidad y establecido procedimientos para el acceso y rectificación de datos personales, promoviendo una cultura de protección de datos en la institución (Transparencia UABC, 2022).

Capurro (2000) sugiere que, para propiciar una cultura digital sólida en Latinoamérica, los latinoamericanos deben crear y difundir esta cultura, teniendo en cuenta los derechos digitales legislados sobre el uso de datos personales, su privacidad y protección. Las bibliotecas públicas y los docentes capacitados pueden ser recursos valiosos para llevar a cabo este enfoque, empoderando a los estudiantes y promoviendo el aprendizaje digital.

La 4RI ofrece una oportunidad para transformar la educación superior y mejorar la formación de profesionales en áreas tecnológicas. Las instituciones educativas deben adaptar sus planes de estudio para incluir competencias digitales y habilidades en ciencia de datos, IA y el internet de las cosas (Orozco, 2019). En Baja California, estudios destacan la importancia de la formación en habilidades digitales para enfrentar los desafíos de la 4RI (Silva-Ayala et al., 2019; Vega-Rivera y Martínez-Rodríguez, 2020). La 4RI y la economía de los datos están impactando la educación superior en Baja California. Las universidades están adaptando sus programas para formar profesionales capaces de enfrentar estos desafíos en un entorno digital y globalizado.

Criterios metodológicos, muestra y metodología

Para evaluar el nivel de conocimiento sobre la protección, uso, aplicación e implicaciones de los datos personales entre los estudiantes de la Facultad de Economía y Relaciones Internacionales (FEyRI) en la UABC, se realizó un análisis documental complementado con una encuesta. Este estudio se enfocó en aspectos éticos y de derechos humanos digitales dentro de la comunidad estudiantil.

En este estudio, los parámetros aplicados fueron: una población de 1395 estudiantes, un nivel de confianza del 95 % ($z = 1.96$), una proporción esperada de éxito ($p = q = 0.5$) y un margen de error del 5 % ($d = 0.05$). Aplicando estos valores en la fórmula, se determinó que el tamaño necesario de la muestra era de 301 estudiantes. Este cálculo fue verificado mediante calculadoras en línea, asegurando la validez y confiabilidad de los resultados.

El instrumento de recolección de datos fue un cuestionario diseñado en Google Forms, que contenía 28 preguntas distribuidas en siete bloques temáticos relacionados con la privacidad y la protección de datos personales. Cada bloque incluía cuatro preguntas de opción múltiple con respuestas “sí”, “no” y “tal vez”, y una pregunta de control de respuesta múltiple con opciones “a”, “b” y “c”. Las respuestas “sí” se consideraron como “informado”, “no” como “no informado” y “tal vez” como “poco informado”. En las preguntas de control, solo la opción correcta se clasificó como “informado”.

El cuestionario cubrió siete temas principales: ética, derechos humanos digitales, regulación, seguridad de datos, protección y privacidad, generación de capacidades y adaptación tecnológica. Para garantizar una alta tasa de respuesta y una correcta aplicación del cuestionario, se realizaron varias acciones de comunicación y coordinación. El cuestionario fue proporcionado a la dirección de la facultad para su aprobación y se contó con el apoyo de autoridades administrativas y docentes para su difusión. Se colocaron hojas con códigos QR en salones y laboratorios, y se publicó la encuesta en la página oficial de Facebook de la FEyRI. Se enviaron correos electrónicos a los estudiantes de posgrado para solicitar su participación.

La encuesta se aplicó en dos rondas. En la primera ronda, se realizó una invitación general en las aulas. En la segunda ronda, programada quince días después, se guio a los estudiantes durante el llenado de la encuesta en tiempo real con el apoyo de los docentes presentes.

Este enfoque permitió obtener una muestra representativa de la población estudiantil, recopilando datos significativos sobre su conocimiento y conciencia en relación con los derechos digitales y la protección de datos personales. Los resultados de la encuesta proporcionaron una base sólida para comprender mejor el ecosistema de protección de datos en la comunidad estudiantil universitaria.

Es importante destacar que se informó a los estudiantes sobre el propósito de la encuesta y la relevancia de sus respuestas. Sin embargo, se decidió no informarles de los resultados individuales para evitar influencias externas que pudieran sesgar sus respuestas. Esta decisión buscó mantener la integridad de los datos obtenidos y asegurar que las respuestas reflejaran el conocimiento en su estado natural.

Las categorías de preguntas en el cuestionario se dividieron en siete bloques temáticos: ética, derechos humanos digitales, regulación, seguridad de datos, protección y privacidad, generación de capacidades y adaptación tecnológica. Cada bloque se diseñó para evaluar un aspecto específico del conocimiento de los estudiantes sobre la protección de datos personales y la privacidad, permitiendo obtener una visión global y completa del nivel de conocimiento de los estudiantes sobre el tema.

El primer bloque, “Ética”, incluyó preguntas para medir el nivel de

conocimiento sobre los valores éticos y las normas de conducta en el manejo de datos personales. El segundo bloque, “Derechos Humanos Digitales”, evaluó la comprensión de los estudiantes sobre los derechos digitales y su relación con la protección de datos personales. El tercer bloque, “Regulación”, se enfocó en el conocimiento sobre las leyes y regulaciones relacionadas con la protección de datos personales. El cuarto bloque, “Seguridad de Datos”, incluyó preguntas sobre aspectos técnicos de la seguridad de datos y las herramientas de protección disponibles. El quinto bloque, “Protección y Privacidad”, midió el conocimiento sobre los conceptos de protección y privacidad de datos personales. El sexto bloque, “Generación de Capacidades”, evaluó las habilidades y competencias necesarias para proteger y gestionar datos personales. Finalmente, el séptimo bloque, “Adaptación Tecnológica”, se enfocó en el conocimiento sobre la adaptación tecnológica y su impacto en la protección de datos personales.

La operacionalización de variables estableció las categorías y preguntas específicas para cada bloque temático, permitiendo medir el nivel de conocimiento de los estudiantes de manera precisa y estructurada. Esta metodología aseguró la recolección de datos relevantes y significativos, proporcionando una base sólida para analizar y comprender el nivel de conocimiento sobre la protección de datos personales y la privacidad en la comunidad estudiantil de la FEyRI.

Para realizar un estudio sobre el conocimiento de la privacidad y protección de datos personales en la Facultad de Economía y Relaciones Internacionales (FEyRI) de la Universidad Autónoma de Baja California (UABC), se implementó una encuesta dirigida a una muestra representativa de estudiantes, tanto de licenciatura como de posgrado. La encuesta incluyó preguntas sobre diversos aspectos relevantes relacionados con los derechos digitales, tales como la nomenclatura de los derechos ARCO, el manejo de datos de menores de edad, la legislación aplicable, los departamentos de derechos digitales, las responsabilidades de las instituciones académicas, la privacidad, la capacitación en derechos digitales y tecnología, y las implicaciones del uso no autorizado de datos personales.

Inicialmente, la muestra consistió en 301 encuestados seleccionados cuidadosamente para garantizar la validez y confiabilidad de los resul-

tados. Sin embargo, para aumentar la precisión, se amplió la muestra en un 11.63 %, resultando en un total de 336 estudiantes encuestados. Esta ampliación permitió obtener una visión más amplia y precisa del conocimiento y percepción de los estudiantes sobre los derechos digitales y su aplicación en el ámbito académico.

Para seleccionar la muestra y llevar a cabo la encuesta, se utilizaron varios canales de comunicación. Primero, se proporcionó el cuestionario a la dirección de la facultad para obtener su consentimiento y autorización. Con el apoyo de la dirección, autoridades administrativas y docentes tanto de posgrado como de licenciatura, se facilitó la aplicación efectiva de la encuesta. Después de una reunión con el subdirector de la facultad, se discutieron los detalles de la aplicación y se difundió la encuesta durante una reunión con los jefes de grupo de la licenciatura. Estos jefes de grupo recibieron un correo con los enlaces para ingresar a la encuesta. Se envió un correo electrónico autorizado por la subdirección, permitiendo el ingreso a las aulas para solicitar a los alumnos que llenaran la encuesta en dos ocasiones.

Se utilizaron diversos medios de comunicación para informar a los estudiantes sobre la encuesta. Se colocaron hojas con el código QR de la encuesta en cada salón de clases y laboratorios de cómputo, con la identificación de contacto y el propósito de la encuesta. También se difundió la encuesta en la página oficial de Facebook de la FEyRI. La Coordinación de Posgrado autorizó la colocación de la hoja con el código QR en las aulas y envió un correo a todos los estudiantes activos de posgrado para solicitar el llenado e informarles del propósito de la encuesta.

La encuesta se aplicó en dos rondas presenciales en las aulas. La primera ronda consistió en una invitación general para que los estudiantes llenaran la encuesta. La segunda ronda, programada quince días después, tuvo como objetivo guiar a los estudiantes durante el llenado de la encuesta en tiempo real, con el apoyo y consentimiento de los docentes presentes.

Esta estrategia permitió obtener una muestra representativa de la población estudiantil de la FEyRI, recopilando datos significativos sobre el conocimiento y la conciencia de los estudiantes en relación con los derechos digitales y la protección de datos personales.

Es importante destacar que se informó a los estudiantes encuestados sobre el propósito de la encuesta y la relevancia de sus respuestas en el estudio. Se les brindó una explicación clara sobre el tema en una charla de diez minutos, asegurando su comprensión de la importancia de su participación en el estudio. Sin embargo, se acordó no informar a los estudiantes de los resultados individuales para evitar influencias externas que pudieran sesgar sus respuestas. Proporcionar una calificación individual podría desmotivar a los estudiantes y, en algunos casos, llevar al desistimiento en el llenado de la encuesta. La divulgación de las respuestas correctas podría influir en la propagación de las mismas o incentivar a los participantes a buscar respuestas en internet, afectando la validez de los datos obtenidos.

Resultados

El objetivo de este estudio fue determinar el nivel de conocimiento sobre la privacidad y protección de datos personales en los estudiantes de FEyRI en el contexto de la 4RI. Donde la tecnología juega un papel crucial en la vida cotidiana y en las relaciones culturales, económicas y sociales, es vital que las personas comprendan los riesgos y desafíos asociados al uso de dispositivos, sistemas y plataformas digitales en cuanto a la privacidad y protección de sus datos personales.

Para evaluar este conocimiento, se llevó a cabo un análisis univariado utilizando frecuencias, estadísticos descriptivos y porcentajes, implementado mediante el programa SPSS. Los resultados obtenidos provienen de las respuestas a 12 preguntas relacionadas con los derechos digitales y la protección de datos personales. La muestra se compuso de 336 estudiantes

Los resultados mostraron que las medias para la mayoría de las preguntas eran relativamente bajas, indicando un conocimiento limitado en temas específicos como la recuperación de inversión por parte de aplicaciones digitales, la correcta nomenclatura de los derechos ARCO y las implicaciones del uso no autorizado de datos personales. Sin embargo, hubo un mayor conocimiento en áreas como la identificación de los derechos digitales como parte de los derechos humanos y la ley que protege la privacidad de los datos personales.

La encuesta también reveló que una proporción significativa de estudiantes no ha recibido capacitación formal sobre sus derechos digitales y

las implicaciones del uso de sus datos personales. Esto subraya la necesidad de implementar programas educativos que fortalezcan la comprensión y conciencia sobre estos temas cruciales en el entorno académico.

Para profundizar en el análisis, se realizó una serie de tablas de frecuencias por pregunta. En la pregunta sobre si los estudiantes conocen cómo las aplicaciones digitales generan beneficios, el 45.5 % respondió afirmativamente, mientras que el 54.5 % no estaban seguros o desconocían este aspecto. Sobre la percepción de los derechos digitales como derechos humanos, el 75.3 % estuvo de acuerdo, lo que muestra una alta conciencia en este ámbito. No obstante, solo el 24.4 % reconoció correctamente que los menores de edad son titulares de sus datos personales, revelando lagunas significativas en este conocimiento.

Respecto a la identificación del departamento universitario encargado de asesorar sobre derechos digitales, el 83 % de los encuestados no tenía conocimiento de su existencia, y solo el 11.3 % afirmó conocerlo. Además, el 56 % de los estudiantes no conocía las responsabilidades de las instituciones académicas en el manejo de datos personales, y un 50.3 % entendió correctamente el concepto de privacidad.

Al examinar la capacitación, el 87.5 % de los encuestados indicó no haber recibido formación sobre derechos digitales, y el 72.9 % no había tomado cursos sobre tecnología y sus implicaciones. Sin embargo, el 53.6 % podía identificar al menos una implicación del uso de sus datos personales sin consentimiento, aunque el 69.3 % identificó incorrectamente las situaciones específicas donde su privacidad podría ser comprometida.

El análisis de los porcentajes de aciertos mostró que la mayoría de los estudiantes tienen un conocimiento “poco informado” sobre privacidad y protección de datos personales, con un promedio de aciertos del 42.99 %. Este resultado sugiere la necesidad de mejorar la educación en estos temas dentro del ámbito universitario.

En el análisis bivariado, se utilizó la prueba t para muestras independientes para identificar diferencias significativas en las respuestas de los estudiantes “informados” y “no informados”. Los resultados indicaron diferencias notables en el conocimiento sobre varios temas, subrayando la importancia de una adecuada educación sobre derechos digitales y protección de datos.

En cuanto a la validación del indicador de nivel de conocimiento (NCPPD), se calculó un valor promedio de aproximadamente 2.97 %, categorizado como “No informado” según la escala establecida. Este resultado confirma la hipótesis de que la comunidad estudiantil necesita fortalecer su conocimiento sobre privacidad y protección de datos en el contexto de la 4RI.

Este estudio destaca la importancia de mejorar la educación y concienciación sobre privacidad y protección de datos personales entre los estudiantes de la FEyRI. Implementar programas de capacitación y formación en estos temas es crucial para empoderar a los estudiantes y prepararlos para enfrentar los desafíos de la era digital de manera segura y responsable.

Conclusiones

Tras el análisis de los resultados de las pruebas estadísticas y la encuesta, se llega a la conclusión de que es necesario mejorar el nivel de conocimiento y habilidades de los estudiantes universitarios de la Facultad de Economía y Relaciones Internacionales de la Universidad Autónoma de Baja California en relación con la protección y privacidad de los datos personales en manos de individuos privados. Aunque se observó que ciertos estudiantes poseen un nivel de conocimiento adecuado sobre estos asuntos, la mayoría evidenció contar con un conocimiento limitado.

Se puede concluir que el nivel de comprensión acerca de las implicaciones de la protección y privacidad de datos personales en los estudiantes universitarios de la Facultad de Economía y Relaciones Internacionales de la Universidad Autónoma de Baja California es limitado. Se sugiere desarrollar un marco teórico que facilite la difusión efectiva de los derechos ARCO y otras herramientas de protección de datos personales tanto en la comunidad universitaria como en la sociedad en general.

Este trabajo presenta una propuesta modesta que puede complementar los resultados obtenidos en diversos contextos. Se centra en un marco exploratorio para la Universidad Autónoma de Baja California, proponiendo que la educación superior sea un espacio para desarrollar capacidades actualizadas acorde a las demandas del entorno digital.

Tanto las instituciones, el Estado y las empresas, como la sociedad deben ser el impulsor de estrategias y acciones que permitan que las tecnologías digitales emergentes se conviertan en herramientas de beneficio y desarrollo integral, promoviendo la prosperidad y el bienestar social en lugar de ser simplemente fuentes de entretenimiento, consumo, dependencia económica y tácticas de marketing.

En la propuesta presentada se expone un marco exploratorio diseñado con el objetivo de disminuir la brecha digital en el ámbito educativo, al mismo tiempo que se promueve una cultura de privacidad y resguardo de la información personal.

El marco propuesto tiene como objetivo facilitar la construcción de capacidades entre el personal administrativo, el cuerpo académico y los estudiantes. Esto se busca con el fin de lograr una adopción equilibrada de tecnología que favorezca la mejora de las operaciones universitarias y permita hacer frente a los desafíos de la Cuarta Revolución Industrial (Kergroach, 2017).

Los resultados obtenidos respaldan la hipótesis inicial de la investigación, la cual plantea la necesidad de fortalecer el conocimiento y las habilidades de la comunidad estudiantil universitaria en relación con la importancia de la privacidad y protección de datos personales. Se sugiere que la Facultad de Economía y Relaciones Internacionales de la Universidad Autónoma de Baja California implemente programas y actividades destinados a promover una cultura y educación digital entre los estudiantes. Asimismo, se propone la difusión clara y accesible de los derechos ARCO y otras herramientas de protección y privacidad de datos personales.

En este campo, los trabajos futuros podrían abarcar la realización de investigaciones adicionales para evaluar la efectividad de los programas y actividades implementados. Asimismo, se propone la exploración de nuevas herramientas y estrategias con el fin de mejorar la educación y concienciación sobre la protección y privacidad de datos personales en posesión de particulares. Sería pertinente comparar los resultados de esta investigación con los de otras instituciones educativas para determinar posibles diferencias significativas en el nivel de conocimiento de los estudiantes sobre estos temas en diversos contextos.

La aplicación de la encuesta en otras escuelas y facultades de la UABC puede ajustarse teniendo en cuenta las características específicas de cada

entorno académico. No obstante, es factible mantener las preguntas referentes al entendimiento de la privacidad y la salvaguarda de información personal, los derechos digitales y otros temas pertinentes. A continuación, se presentan algunas pautas a considerar para llevar a cabo la encuesta en dichas instituciones:

Para garantizar la pertinencia y adecuación de la encuesta a la institución educativa correspondiente, se aconseja la revisión y adaptación de la encuesta original. Se sugiere mantener las preguntas sobre derechos digitales, privacidad y protección de datos personales, aunque es factible introducir cambios o añadir preguntas de acuerdo con las particularidades específicas de la escuela o facultad en cuestión.

Es fundamental llevar a cabo una revisión minuciosa y validar el contenido de la encuesta antes de su aplicación en distintas escuelas o facultades. Esto requiere garantizar la claridad, comprensibilidad y relevancia de las preguntas para los estudiantes de cada institución específica.

Para garantizar la validez de los resultados, es necesario llevar a cabo un proceso de selección de muestra representativa, similar al mencionado anteriormente. Este procedimiento implica establecer criterios para seleccionar a los participantes, tales como su nivel educativo (secundaria, preparatoria, licenciatura, posgrado) y la facultad o escuela a la que pertenecen, entre otros aspectos.

La comunicación y difusión son aspectos fundamentales para informar a los estudiantes sobre la encuesta y motivar su participación. Es esencial establecer canales de comunicación apropiados, como el correo electrónico, las redes sociales institucionales, los sitios web y los anuncios en aulas. Se debe garantizar la claridad en la información proporcionada acerca del propósito de la encuesta, su relevancia y la confidencialidad de las respuestas.

La aplicación de la encuesta puede seguir una metodología que se asemeje al enfoque previamente descrito. Se puede considerar la posibilidad de llevar a cabo una presentación inicial para situar a los estudiantes en el contexto del tema y para explicar los objetivos de la encuesta. Es recomendable emplear un método anónimo con el fin de asegurar la confidencialidad de las respuestas y prevenir posibles influencias externas.

Es fundamental considerar que cada unidad académica de la UABC puede contar con sus propias pautas y exigencias particulares. Por consi-

guiente, se aconseja coordinar con las autoridades y encargados de cada entidad con el fin de ajustar el enfoque de implementación de la encuesta conforme a las directrices y normativas vigentes.

En síntesis, la extensión de la encuesta a otras instituciones académicas de la Universidad Autónoma de Baja California requiere la adecuación del cuestionario, la implementación de una comunicación eficaz, la salvaguarda de la confidencialidad de las respuestas y el seguimiento de una metodología acorde a las características específicas de cada entidad educativa.

Para hacer frente a los desafíos de la sociedad digital en constante evolución, es esencial comprender las implicaciones de la privacidad y la importancia de proteger los datos personales. Se requiere la implementación de acciones e iniciativas que conciencien a la población sobre los beneficios, la naturaleza y el impacto de la digitalización en la vida diaria. Asimismo, es crucial desarrollar, implementar y evaluar de manera continua programas educativos y de capacitación para mitigar los posibles daños causados por los efectos perniciosos de las tecnologías exponenciales. Expertos y académicos en ética de la IA, como Cortina (2021), Zuboff (2020), Lee (2019) y Jasanoff (2016), han destacado la importancia de esta labor.

En el proceso de reflexión y análisis acerca de los límites de la digitalización y el futuro de la sociedad digital, se considera que aspectos como la brecha digital, la protección de datos, la privacidad, la confidencialidad y la certidumbre son de vital importancia. Asimismo, se destaca la relevancia de aspectos éticos y morales, los procedimientos de ciberseguridad, así como la regulación por parte de los Estados y organismos internacionales. La falta de atención a estos factores fundamentales pone en riesgo el futuro de la sociedad digital. En este contexto, el sector educativo desempeña un papel crucial en la transición de la sociedad hacia la Cuarta Revolución Industrial, promoviendo valores sociales y objetivos compartidos que buscan garantizar una vida digna y bienestar en el actual entorno digital (Tegmark, 2018).

Según lo expuesto por Schwab (2016)

Al reflexionar sobre la manera de aprovechar la revolución tecnológica, se promueve la autoevaluación y el análisis de los modelos sociales implícitos en estas tecnologías, lo que a su vez brinda la posibilidad de influir en la revolución de forma positiva para mejorar la situación global (p.13).

Referencias

- Capurro, R. (2000). Ética de la información en América Latina. *Revista de Ética y Deontología*, 2(2), 15-30.
- Cate, F. H. (2019). The privacy problem: Strategies for solutions. *Journal of Law, Technology & Policy*, (2), 105-142.
- Cortina, A. (2022). Ética cosmopolita y datos personales: Una mirada crítica a la vigilancia. *Revista de Filosofía*, 67(3), 295-318.
- De Hert, P. y Gutwirth, S. (2009). *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*. Springer.
- García Macías, J. A. (2019). Composición de políticas basada en el contexto de uso de datos. *Ingeniería, Investigación y Tecnología*, 20(2), 129-144.
- González Guerrero, L. D. (2019). Control de nuestros datos personales en la era del big data: El caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, 21(1), 55-72.
- Hernández-Fuentes, J. L., & Ortiz-López, J. J. (2020). La educación superior ante los desafíos de la Cuarta Revolución Industrial: Reflexiones desde la perspectiva de la ética y la responsabilidad social. *Revista Mexicana de Investigación Educativa*, 25(87), 329-352.
- ISTE. (2017). *Standards for students*. International Society for Technology in Education. <https://www.iste.org/standards/for-students>
- Kang, S., & Stein, M. (2019). Digital rights as human rights: The perspectives of university students. *Journal of Human Rights*, 18(3), 287-305.
- Kergroach, S. (2017). Industry 4.0: New challenges and opportunities for the labour market. *OECD Science, Technology and Industry Policy Papers*, (53). OECD Publishing.

- Lee, K. F. (2020). *AI Superpowers: China, Silicon Valley, and the New World Order*. Houghton Mifflin Harcourt.
- Martínez Devia, J. (2019). La protección de datos personales en el entorno digital: Retos y perspectivas. *Revista de Derecho Informático*, 15(2), 175-192.
- NCES. (2018). *Data protection in education: Recommendations for schools*. National Center for Education Statistics. <https://nces.ed.gov>
- OECD. (2015). *Students, Computers and Learning: Making the Connection*. PISA, OECD Publishing.
- Orozco, M. (2019). Transforming higher education in the digital age: Challenges and strategies. *Journal of Educational Change*, 20(4), 563-578.
- Piñar Mañas, J. L. (2010). ¿Existe la privacidad? *Revista Española de Protección de Datos*, 4(1), 10-28.
- Prabhakara, G. (2021). Understanding data privacy in the age of digital transformation. *Information Management Journal*, 55(3), 210-225.
- Prieto-Santana, J. et al. (2019). Data protection in higher education: Student awareness and practices. *Journal of Educational Technology*, 45(2), 175-189.
- Ramírez-Alvarez, M., Rodríguez-Gómez, G., & Vázquez-Cano, E. (2020). ¿Cómo protegen los usuarios sus datos personales en redes sociales? Un estudio de caso en México. *El profesional de la información*, 29(3), e290302.
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.
- SEP. (2020). *Estrategia Digital Nacional para la Educación*. Secretaría de Educación Pública. <https://www.sep.gob.mx>
- Serrano-Santoyo, A. (2018). Retos de la protección de datos personales en México. *Cuadernos de Información*, 32(2), 85-99.
- Silva-Ayala, M., et al. (2019). Formación en competencias digitales para la 4RI en Baja California. *Revista Iberoamericana de Educación*, 79(1), 77-92.
- Tapscott, D., & Osorio, M. B. (1997). *La economía digital*. McGraw-Hill.
- Tegmark, M. (2018). *Vida 3.0: Ser humano en la era de la inteligencia artificial*. Debate.

- Tenorio Cueto, G. A. (2019). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares, comentada*. Editorial Porrúa.
- Tenorio, G. A. (2021). *Desafíos de la privacidad en la era digital*. Editorial Porrúa.
- Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.
- UNESCO. (2015). *Replantear la educación: ¿Hacia un bien común mundial?* Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. <https://unesdoc.unesco.org/ark:/48223/pf0000232555>
- US Department of Education. (2019). *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. <https://studentprivacy.ed.gov>
- Vega-Rivera, B., & Martínez-Rodríguez, J. (2020). Desafíos y oportunidades de la 4RI para la educación superior en Baja California. *Revista de Educación Superior*, 50(198), 113-130.
- Véliz, C. (2021). *Privacidad es Poder*. Debate.
- Zuboff, S. (2020). *La era del capitalismo de la vigilancia*. Paidós.

