Seguridad y Privacidad en la gestión de Datos Académicos en las Escuelas (SPADATAS)

2022-1-ES01-KA220-SCH-000086363

SPADATAS

Security and Privacy in Academic Data Managment at Schools

Co-funded by the European Union

Privacidad de datos de estudiantes en la era de la Inteligencia Artificial

HUMAN ENVIRONMENT RESEARCH GROUP – TECHNOLOGY ENHANCED LEARNING Universitat Ramon Llull (URL) – Universidad de Salamanca (USAL)

SPADATAS CONSORTIUM

2024

Recuerde Proteger, Salvaguardar y Prevenir Riesgos para la Privacidad de los Datos de los Estudiantes

- **Protección contra acceso no autorizado**
  La confidencialidad de la información de los estudiantes es crucial. Por lo tanto, mantenga seguros los nombres, números de seguro social, calificaciones y otros datos personales.
- **Protección contra el cibercrimen**
  Previene el robo de identidad y otras formas de delitos cibernéticos al proteger la información personal.
- **Prevención de ataques/discriminación injustos**
  Mantiene la justicia y la equidad al mantener la confidencialidad de los datos de los estudiantes, evitando así el uso indebido con fines de discriminación o colocación académica injusta.

La coherencia es esencial cuando se trata de salvaguardar información confidencial. Las actualizaciones periódicas de software/hardware y las auditorías de seguridad ayudan a garantizar la seguridad continua de los sistemas. Esto implica mantener actualizados el software antivirus y los firewalls y realizar auditorías de seguridad de rutina. Además, la implementación de protocolos de contraseña robustos, autenticación de dos factores y cifrado de datos durante los procesos de transmisión y almacenamiento mejora notablemente la seguridad. Al fomentar el uso de contraseñas complejas y únicas y al mismo tiempo promover cambios regulares, las instituciones educativas agregan capas de protección adicionales a sus sistemas.

Tener políticas y procedimientos bien definidos para el manejo de datos es crucial. Las instituciones educativas deben definir claramente quién tiene acceso a los datos de los estudiantes, especificar los usos permitidos y establecer pautas para el almacenamiento y la protección. Por este motivo, la formación periódica del personal docente sobre estas materias es fundamental para cultivar una cultura de conocimiento de la privacidad. Por lo tanto, las instituciones educativas deben cumplir con regulaciones como el Reglamento General de Protección de Datos (GDPR) y mantener políticas de privacidad de fácil acceso para todas las partes interesadas.

Es fundamental preservar la privacidad de los datos y evitar cualquier uso indebido de su información. Las instituciones educativas deben participar de manera proactiva en esfuerzos para fortalecer la seguridad de los datos de los estudiantes, creando un entorno de aprendizaje seguro y protegido. Todo esto se aplica a la era de la inteligencia artificial.

Privacidad de los datos de los estudiantes en la era de la inteligencia artificial (IA)

La integración de la Inteligencia Artificial (IA) en la educación ha abierto nuevas vías para mejorar las metodologías de aprendizaje y enseñanza. Las herramientas basadas en IA pueden personalizar las experiencias de aprendizaje, automatizar tareas administrativas y proporcionar información

Co-funded by the European Union

El proyecto SPADATAS (Ref.: 2022-1-ES01-KA220-SCH-000086363) está cofinanciado por el programa Erasmus+ de la Unión Europea. El contenido de esta publicación es responsabilidad exclusiva del consorcio y ni la Comisión Europea, ni el Servicio Español para la Internacionalización de la Educación (SEPIE) son responsables del uso que pueda hacerse de la información aquí divulgada.

valiosa sobre el desempeño de los estudiantes. Sin embargo, esta innovación también trae consigo importantes desafíos, especialmente en lo que respecta a la privacidad de los datos de los estudiantes.

1. **Mayor recopilación y procesamiento de datos**

Los sistemas de IA dependen en gran medida de los datos para funcionar de forma eficaz. En entornos educativos, estos sistemas recopilan y procesan grandes cantidades de datos confidenciales de los estudiantes, incluidos identificadores personales, registros académicos y, a veces, datos biométricos. Esta extensa recopilación de datos genera preocupaciones sobre la posibilidad de violaciones y uso indebido de la privacidad.

2. **Riesgo de violaciones de datos y amenazas de ciberseguridad**

Los sistemas de IA, como cualquier tecnología digital, son susceptibles a ciberataques y filtraciones de datos. Las consecuencias de tales incidentes en contextos educativos son particularmente graves, dada la sensibilidad de los datos de los estudiantes. El acceso no autorizado a estos datos puede provocar robo de identidad, chantaje y otras formas de delitos cibernéticos que afecten a los estudiantes y sus familias.

3. **Perfiles de datos y sesgos involuntarios**

Los algoritmos de IA pueden conducir inadvertidamente a la elaboración de perfiles de los estudiantes en función de sus datos, lo que podría afectar sus oportunidades académicas y profesionales. También existe el riesgo de que los sistemas de inteligencia artificial perpetúen y amplifiquen los sesgos de sus datos de capacitación, lo que lleva a prácticas educativas injustas o discriminatorias.

4. **Cuestiones de transparencia y rendición de cuentas**

Muchos sistemas de IA funcionan como "cajas negras", con procesos de toma de decisiones que son opacos para los usuarios. Esta falta de transparencia puede dificultar que los educadores y administradores comprendan cómo se utilizan los datos de los estudiantes y garanticen la responsabilidad en caso de errores o uso indebido.

5. **Cumplimiento de la Normativa de Protección de Datos**

El uso de IA en la educación debe cumplir con las leyes de protección de datos como el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad y Derechos Educativos de la Familia (FERPA) u otras regulaciones regionales. Las escuelas y las instituciones educativas enfrentan el desafío de alinear las prácticas de IA con estos marcos legales para garantizar el manejo legal y ético de los datos de los estudiantes.

6. **El uso ético de la IA en la educación**

Los educadores y proveedores de tecnología deben priorizar el uso ético de la IA, garantizando que los datos de los estudiantes se utilicen únicamente para mejorar la experiencia educativa y no con fines comerciales u otros fines inapropiados. Esto incluye obtener el consentimiento informado para la recopilación y el procesamiento de datos, garantizar la transparencia y respetar la privacidad y los derechos de los estudiantes.

Co-funded by the European Union

El proyecto SPADATAS (Ref.: 2022-1-ES01-KA220-SCH-000086363) está cofinanciado por el programa Erasmus+ de la Unión Europea. El contenido de esta publicación es responsabilidad exclusiva del consorcio y ni la Comisión Europea, ni el Servicio Español para la Internacionalización de la Educación (SEPIE) son responsables del uso que pueda hacerse de la información aquí divulgada.

Conclusión

A medida que la IA se vuelve cada vez más frecuente en los entornos educativos, no se puede subestimar la importancia de la privacidad de los datos de los estudiantes. Los educadores, administradores y proveedores de tecnología deben trabajar en colaboración para establecer protocolos sólidos de privacidad de datos, promover la transparencia y defender estándares éticos en el uso de la IA. Al hacerlo, pueden aprovechar los beneficios de la IA en la educación y al mismo tiempo salvaguardar la privacidad y seguridad de los datos de los estudiantes.

Puntos clave:

1. **Protección de datos**: Mantener la confidencialidad de los nombres de los estudiantes, números de seguro social, calificaciones y otros datos personales.
2. **Medidas de seguridad**: implementación de protocolos de contraseñas seguras, autenticación de dos factores, actualizaciones periódicas del sistema y políticas transparentes de manejo de datos.
3. **Medidas proactivas**: las escuelas deben trabajar activamente para proteger los datos de los estudiantes, garantizando un entorno de aprendizaje seguro.
4. **Formación y concienciación**: educar al personal sobre la privacidad y seguridad de los datos.
5. **Capacidades de IA**: la inteligencia artificial (IA) puede procesar y analizar con precisión grandes cantidades de datos, pero también existe el riesgo de un posible uso indebido de los datos de los estudiantes a través de la tecnología de IA.
6. **Preocupaciones sobre la privacidad de los datos**: se destacan los riesgos relacionados con las violaciones de la privacidad de los datos, el acceso no autorizado a los datos y el uso indebido.
7. **Uso ético**: una guía sobre consideraciones éticas y uso responsable de la IA en el aula es crucial
8. **Cumplimiento**: asegúrese de que las herramientas de inteligencia artificial cumplan con las regulaciones de protección de datos como GDPR. Mantener la política de privacidad accesible para los profesores.
9. **Mejores prácticas**: los profesores deben tener directrices para incorporar de forma segura herramientas de IA en las prácticas educativas y sus implicaciones para la seguridad de los datos.
10. **Actualizaciones y monitoreo**: Mantenga los sistemas de IA actualizados y monitoreados para detectar vulnerabilidades de seguridad.

Co-funded by the European Union

El proyecto SPADATAS (Ref.: 2022-1-ES01-KA220-SCH-000086363) está cofinanciado por el programa Erasmus+ de la Unión Europea. El contenido de esta publicación es responsabilidad exclusiva del consorcio y ni la Comisión Europea, ni el Servicio Español para la Internacionalización de la Educación (SEPIE) son responsables del uso que pueda hacerse de la información aquí divulgada.