Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II (Gpo 501)

Privacidad y Seguridad de los Datos

Adrián Emmanuel Faz Mercado - A01570770

Octubre 28, 2023

Cuando se trabajan con datos relacionados con información personal de individuos, es de suma importancia garantizar la protección y confidencialidad de esa información, al igual que estar consciente de cuál es el tipo de datos que se están manejando y conocer las normativas correspondientes.

En el caso de nuestro reto, estamos trabajando con un sistema de detección de asistencia y participación de estudiantes en el aula, el cual, si bien puede ser una excelente herramienta para automatizar procesos y mejorar la eficiencia educativa, también conlleva una gran responsabilidad en cuanto a la gestión y protección de datos.

En el reto, los datos sensibles de los estudiantes que se están manejando son los nombres completos de los estudiantes y sus fotografías. Esto puede ser peligroso en caso de que exista una manera en la que se pueda relacionar la imagen de la persona con su nombre. Si se manejan de forma individual y aislada, los datos pueden no representar un riesgo inmediato para la privacidad, pero cuando se combinan, correlacionan o se integran en sistemas más amplios, tienen el potencial de crear perfiles detallados de individuos. Estos perfiles pueden ser utilizados para identificar, rastrear o incluso realizar una suplantación de identidad de las personas. Es necesario anonimizar los datos, y por esto, en nuestro equipo de trabajo decidimos que en vez de relacionar la cara directamente con el nombre de la persona y enviar esto a la base de datos, se utilizará un **ID único** para identificar a los estudiantes, el cual será generado de manera aleatoria y no tendrá ninguna relación directa con la información personal del estudiante. De esta manera, incluso si alguien accediera de manera no autorizada a la base de datos, no podría relacionar de inmediato las imágenes con los nombres o cualquier otro dato sensible de los estudiantes.

En México, la normativa actual que aplica para el reto que se presenta es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual es la principal normativa en México que regula cómo las entidades privadas deben manejar y proteger los datos personales que tienen en su posesión. Esta ley aplica a TODAS las personas físicas o morales de carácter privado, que en el desarrollo de sus actividades traten datos personales. (INAI, 2016). En esta normativa, se explican diferentes principios que deben de ser cumplidos por las entidades que manejen datos personales, que en este caso, sería la escuela/empresa que se encarga de administrar el sistema de detección de asistencia y participación. Debemos de verificar que estos principios se cumplan para así asegurar que los datos (nombres y fotografías) de los estudiantes estén protegidos.

Uno de estos principios es el del consentimiento, el cual establece que cualquier tratamiento de datos personales requiere de la autorización previa e informada de la persona a quien pertenecen los datos. Es decir, antes de recopilar la información personal de alguien, esa persona debe estar totalmente informada de cómo se usarán sus datos y dar su permiso explícito para ello. En nuestro caso, para cumplir con este principio, antes de que se implemente el sistema de detección en cualquier escuela, será necesario que los estudiantes, o en el caso de menores de edad, sus tutores o representantes legales, firmen un documento o formulario de consentimiento. En este documento, se detallaría de manera clara el objetivo

del sistema, cómo se procesarán y almacenarán los datos, y también las medidas de seguridad implementadas para proteger su privacidad. De igual forma, se explicará que las imágenes y los nombres solo se utilizarán con el propósito de registrar asistencia y participación, sin ser compartidos o usados para otros fines. Con esto, también se ve involucrado el principio de la Información, el cual establece que por ley, el titular debe de recibir toda la información relevante sobre cómo, por qué y para qué se usarán sus datos, normalmente a través del aviso de privacidad. Para el sistema de detección, se elaborará un aviso de privacidad detallado, que se les proporcionará a los estudiantes y a sus tutores en caso de que sean menores. Este documento incluirá información sobre el responsable del tratamiento de los datos, los las maneras en las que se recolectará y procesará la información, cuánto tiempo va a estár almacenada la información, y los derechos que tienen los estudiantes y los tutores sobre sus datos, incluyendo el acceso, rectificación, cancelación y oposición. (Sus derechos ARCO)

Ahora, es esencial que se cuente con un proceso de validación del manejo de los datos y garantizar que únicamente el equipo tenga acceso a ellos. Este proceso inicia con la asignación de roles específicos relacionados con la gestión de los datos y las actividades que puede realizar. Cada rol tiene permisos claramente definidos que limitan o permiten el acceso a ciertas áreas o funciones del sistema, garantizando así que los datos no sean manipulados o vistos por personas que no están autorizadas. En nuestro caso, estaríamos contando con 4 roles principales, los cuales son estudiante, docente, administrador y desarrollador. El estudiante tendrá acceso solamente para revisar su propia asistencia y participación, pero no tendrá la capacidad para modificar o accesar a los datos de otros estudiantes. El docente tendrá acceso a los registros de asistencia y participación de los estudiantes de sus respectivas clases o materias. Podrán ver las estadísticas únicamente de sus grupos para así evaluar la participación y presencia en sus clases, pero no podrán realizar ninguna modificación directamente los registros sin antes pasar por alguna validación ni tendrán acceso a los datos de estudiantes que no son de sus clases. El rol de administrador es mucho más amplio y tiene permisos para gestionar usuarios, crear y modificar cursos, asignar roles y realizar tareas administrativas. Finalmente, el rol de desarrollador tiene acceso tanto al código fuente como a la base de datos para realizar actualizaciones, correcciones y mejoras en el sistema, pero está limitado solamente a las personas que están trabajando actualmente en la plataforma.

Esta división clara de roles permite que cada persona interactúe con el sistema de acuerdo con sus responsabilidades y necesidades específicas, logrando así que se minimicen los riesgos de acceso no autorizado o uso indebido de la información. Además de ello, para garantizar la seguridad y autenticidad del acceso, se implementará un sistema de inicio de sesión con autenticación de dos factores (2FA). Esto permitirá que se añada una capa adicional de protección contra posibles ataques como el phishing o el robo de credenciales. Incluso si una persona obtuviera la contraseña de un usuario, no podrá acceder al sistema sin superar el segundo nivel de autenticación.

Otra parte importante de este proceso de validación que solo el equipo tenga acceso a estos datos es asegurarse de que las contraseñas sean generadas de manera segura. Para ello, el

sistema requerirá que las contraseñas cumplan con ciertos criterios para ser consideradas válidas. Esto incluye una longitud mínima (8 caracteres), la combinación de letras mayúsculas y minúsculas, números y símbolos especiales. Igualmente, el sistema no permitirá que se utilicen contraseñas comunes o que sean fácilemnte adivinables. Finalmente, para reforzar aún más la seguridad, el sistema contará con medidas contra intentos repetidos de inicio de sesión fallidos, lo cual bloquearía temporalmente la cuenta después de que exista cierto número de intentos fallidos. Esto ayuda a proteger contra ataques de fuerza bruta, donde los atacantes intentan adivinar la contraseña probando muchas combinaciones diferentes.

Finalmente, para llevar un control del acceso y la manipulación de los datos, se implementará un mecanismo que permita rastrear los movimientos y los usuarios que realizaron cada acción. Este mecanismo registrará todo intento de acceso, tanto exitoso como fallido, lo cual indicará quién intenta acceder al sistema y cuándo. Además, cada acción que se realice con los datos, ya sea sea crear, leer, actualizar o eliminar también deberá ser registrada con un sello de tiempo. Se registrará el nombre del usuario, el rol y la dirección IP desde donde se realizó el acceso. Regularmente, se llevarán a cabo auditorías internas en las que se examinarán y revisarán los registros de acceso para identificar si existe algún patrón inusual o actividades sospechosas. Estas auditorías se realizarán por un equipo especializado que tiene como principal objetivo garantizar el cumplimiento de las normativas de protección de datos y la integridad del sistema.

La implementación del sistema de detección de asistencia y participación tiene muchos beneficios, pero también representa una gran responsabilidad, por lo que es crucial asegurar un manejo ético y seguro de los datos personales de los estudiantes. La implementación de protocolos robustos, la asignación clara de roles y el monitoreo constante son esenciales para mantener la confianza y proteger la privacidad de los usuarios. Al cumplir con las normativas vigentes y al añadir capas adicionales de seguridad, no solo se protege la información de los estudiantes, sino que también se fortalece la integridad y confiabilidad del sistema. Definitivamente, proteger la privacidad y la seguridad de los datos no es solamente una obligación legal, sino una responsabilidad moral que permite garantizar el respeto y la confianza del uso de tecnologías en la educación.

Referencias bibliográficas

1. INAI (2016) Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Recuperado el 24 de Octubre del 2023, de: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf

2. Cámara de Diputados del Congreso de la Unión. (2011) REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. Recuperado el 24 de Octubre del 2023, de: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf