



Tecnológico de Monterrey

Campus Querétaro

Asignatura

Inteligencia artificial avanzada para la ciencia de datos

Proyecto

Privacidad y Seguridad

Frida Lizett Zavala Pérez

A01275226

8 de Noviembre del 2023

Inteligencia artificial avanzada para la ciencia de datos

El inicio de cualquier proyecto, especialmente cuando involucra la colaboración con empresas de renombre como General Electric (GE), no solo implica aprender cuestiones técnicas para resolver el reto propuesto, sino también una serie de acuerdos fundamentales que establecen las bases para una colaboración efectiva y ética. En este sentido, recientemente hemos comenzado un proyecto en el que se han generado importantes discusiones entre los equipos legales del ITESM y GE, con el objetivo de forjar un acuerdo que beneficie a ambas partes, tomando como una de las prioridades la protección del bienestar y derechos de los estudiantes y, al mismo tiempo, resguarde la integridad, confidencialidad y propiedad intelectual de los datos suministrados por la empresa.

El punto principal de este acuerdo reside en el suministro de datos por parte de GE, específicamente reportes sobre el comportamiento de turbinas en vuelos comerciales. No obstante, la sensibilidad y confidencialidad de estos datos son prioritarias. Por ende, se ha llevado a cabo un minucioso proceso de anonimización por expertos en ciencia de datos de la empresa, utilizando técnicas avanzadas para crear representaciones significativas sin comprometer la privacidad de la información original, sin embargo no se descarta la posibilidad de que alguno de los perfiles de vuelo simulados no se apeguen a la realidad en su totalidad. Esto, a su vez, ha generado un ambiente de confianza en el que se puede trabajar de manera responsable con estos datos sin temor a vulnerar la privacidad de los involucrados, en este caso los clientes de la empresa.


Dado que los reportes de vuelo como se mencionó anteriormente pertenecen a simulaciones basadas en vuelos comerciales de diversos clientes de GE, es necesario proteger esa información, es por ello que se realizaron dichos procedimientos para generar la base de datos. Ahora bien, a pesar de que los datos proporcionados no revelan información sensible de ninguno de los vuelos reales, éstos al haber sido procesados por las personas de GE, son propiedad de la empresa, por lo que debe protegerse también la propiedad intelectual de los mismos y no pueden ser distribuidos de manera libre. GE, como entidad comprometida con la privacidad y la protección de su propiedad intelectual, ha implementado estrictos procesos de seguridad para garantizar que se cumplan las normativas que salvaguardan la integridad de los datos suministrados.

Para General Electric la privacidad tanto de los datos como de los clientes es un tema importante, así como la protección de propiedad intelectual, por lo que cuentan con diversos procesos para garantizar que se cumplan las reglas y parámetros que salvaguarden la integridad de los mismos. Una guía de comportamiento y valores de la empresa por la que se rigen sus integrantes es su código de conducta: “The spirit and the letter”, documento donde se estipula por escrito dichas reglas y acuerdos, teniendo un apartado en la página 16 dedicado a la propiedad intelectual, donde se especifica que se debe actuar bajo la ética y el respeto, así como el no difundir información de la empresa a terceros sin un previo consentimiento y acuerdo de por medio.

El acceso a los datos se encuentra limitado únicamente a la computadora proporcionada por la empresa, éstos se encuentran alojados en box medio por el cuál se nos compartieron, se realizó la sincronización al equipo y posteriormente se descargaron de manera local. Ya que el acceso a los datos es únicamente a través del equipo de la empresa y, estos no pueden ser distribuidos ni compartidos de ninguna manera; están destinados únicamente para desarrollar el proyecto y las acciones del equipo se encuentran monitoreadas por los métodos y configuraciones con las que ya cuenta previamente la computadora. Se recibe alertas en caso de que se intente sacar algún dato de la computadoras, esto implica que los puertos USB se encuentran bloqueados y que no es posible enviar archivos a través de correo, ni abrir servicios como WhatsApp, enviar imágenes de capturas de pantalla, o subir archivos a repositorios desde el equipo. Además, debido a los bloqueos con los que se cuenta en la red de Tec, es necesario utilizar una red externa con la finalidad de prevenir cualquier intento no autorizado de transferencia de datos. Asimismo, solo se permiten herramientas aprobadas por GE para manipular dichos datos, manteniendo un control riguroso sobre su uso. Cabe mencionar que para acceder y poder hacer uso de la computadora es necesario contar con las credenciales y contraseñas configuradas especialmente para cada equipo las cuales solo están disponibles para los miembros del equipo y profesores.

Las computadoras se mantienen bajo resguardo del almacén del edificio de electrónica del ITESM y únicamente los integrantes del equipo pueden acceder a ellos bajo supervisión de los profesores del bloque, su espacio de uso se limita al salón de clase donde se imparte el curso, en un horario de 7am a 2 pm, lo cual nos provee más control sobre lo descrito anteriormente. Se ha propuesto un registro manual que documente quién es responsable de la

computadora, cuándo y bajo qué condiciones, dónde se registrará la hora de acceso y la hora de entrega de la computadora, para tener un control y registro del acceso a los datos, además de que se cuenta con el registro del almacén sobre cuándo se ha pedido y entregado la computadora. Se asume que al acceder a la computadora se le atribuye el cargo a un miembro del equipo, sin embargo el acceso a el mismo se extiende a los miembros del equipo durante las horas de trabajo registradas, para realizar actividades meramente del reto.

Bitácora de acceso:  Seguimiento

Este contexto nos lleva a reflexionar sobre la importancia de la ética y responsabilidad al trabajar con datos suministrados por entidades externas. La necesidad de proteger la confidencialidad, propiedad intelectual y privacidad, aun cuando los datos parezcan no revelar información sensible, se convierte en un punto crucial para salvaguardar la integridad de la información y la confianza en colaboraciones futuras.

En consecuencia, todos los participantes, desde profesores hasta estudiantes, han firmado un acuerdo de confidencialidad al inicio del proyecto. Este acto no solo simboliza el compromiso con los términos acordados, sino que también refuerza la importancia de la transparencia, la ética y la responsabilidad en la manipulación de datos suministrados por entidades externas. Este proyecto representa una oportunidad no solo para el desarrollo técnico y académico, sino también para la reflexión sobre la responsabilidad y ética al trabajar con datos proporcionados por empresas, estableciendo un marco de trabajo que garantice la integridad, privacidad y propiedad intelectual.

Referencias

General Electric (2023). Código de conducta. The spirit and the letter. Recuperado de. <https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf>