

# **Actividad Ética y Computación**

## **Situación 1:**

### **Principios de Privacidad en el Código ACM de Ética:**

Los artículos que hablan sobre la privacidad en el Código de ética de ACM establecen lo siguiente:

- 1.03. *Aprobar el software solo si tienen un pozo creencia fundada de que es seguro, cumple con las especificaciones, pasa las pruebas apropiadas y lo hace. No disminuye la calidad de vida, disminuir la privacidad o dañar al ambiente. El efecto final del trabajo debe ser para el bien público.*
- 3.12. *Trabajar para desarrollar software y documentos relacionados que respeten. La privacidad de aquellos que se verán afectados por ese software.*

### **Descripción de la situación:**

Una empresa que ofrece gestión de pagos tiene un desarrollador de backend que trabaja en la API para dicho gestor de pagos. El tiene un fecha de vencimiento de 2 semanas antes del lanzamiento de la primera versión del API al público, pero él sabe que implementando el tipo de cifrado para NPI (formación personal no pública) que el GLBA demanda tomarán al menos un mes.

Para quitar el problema de las manos y cumplir con la fecha de vencimiento, él decide cifrar solo con SHA256 la información pública del usuario y dejar el NPI sin cifrar durante las transacciones, pero en un canal "seguro" que simplemente "parece" seguro. La API es aprobada por sus superiores no técnicos y se estrena a tiempo.

Dos semanas después, el gobierno cita a la compañía e inicia una investigación en más de 40,000 cuentas bancarias fácilmente robadas por un grupo de hackers debido a la baja seguridad del API de la compañía. La compañía ahora enfrenta demandas de millones de dólares y perdió su reputación para siempre, impidiéndole volver a operar. Todo solo por un desarrollador de encaje que decidió no proteger la privacidad de sus usuarios.

### **Solución:**

Siempre es mejor posponer una fecha de vencimiento para garantizar una parte crítica de un desarrollo que lanzar un producto no terminado. Es siempre más costoso arreglar algo que ya es público especialmente en temas de seguridad que involucran la información del usuario.

## **Situación 2:**

### **Principio 4: JUICIO**

- 4.03. Mantener la objetividad profesional con respecto a cualquier Software o documentos relacionados que se les pide evaluar.

- 8.07 No dar trato injusto a nadie por irrelevante. prejuicios

### **Caso de negocio:**

Recientemente ha habido muchos problemas con respecto a la IA (Artificial Inteligencia) siendo racista debido a los conjuntos de datos bajo los cuales se están desarrollando y aprendiendo.. Desde el software de la cámara (Nikon) que reconoce a los asiáticos como que siempre están parpadeando, hasta los sistemas de clasificación policial etiquetando africano-americanos como "criminales potenciales" sobre los caucásicos.

Posiblemente podamos acreditar esto al origen de la mayoría de los conjuntos de datos utilizados para entrenar redes neuronales: Estados Unidos. Más del 45% de la ImageNet (un dataset de imagen masiva comúnmente utilizado para entrenamiento) proviene de Estados Unidos, mientras que Asia solo contribuye con el 4% de los datos. Esta falta de geodiversidad explica en parte por qué los algoritmos de hoy tienden a ser racistas.

### **Solución:**

Es nuestra obligación como ingenieros de software asegurar que nuestros productos tanto como nuestro juicio está libre de prejuicios, que es ¿Por qué debemos asegurarnos de que nuestros conjuntos de datos sean equilibrados y ricos en diversidad para evitar cualquier malentendido en los algoritmos que desarrollamos.

## **Reflexión**

Nosotros vamos a crecer a ser personas que manejan cantidades gigantescas tanto de información pública como privada. También seremos nosotros quien dotemos de inteligencia a las futuras máquinas. Y por todo esto y más, nosotros cargamos con una gran responsabilidad, y es por esto que debemos apegarnos a un código de ética.

Por lo que hemos estudiado del código de ética del ACM. Si todos nosotros, todos los ingenieros, y todas las empresas trabajan apegados a este código de Ética no

estaríamos viendo los escándalos que estamos teniendo, no tendríamos que preocuparnos que tanto escondemos nuestra información, podríamos confiar en las empresas con más facilidad, y en general sería un mundo ideal por lo que es esto probablemente nunca suceda.

El código de ética de la ACM es algo por lo que nos debemos de regir todos y es muy importante seguir estudiando, aprendiendo, y entendiendo todos sus artículos para evitar caer en malas prácticas al momento de estar desarrollando nuestros futuros productos.