BIG DATA APLICADA A UN MODELO PREDICTIVO PARA IDENTIFICAR DELITOS DE ACOSO EN LA RED SOCIAL FACEBOOK

LEYNA ROXANA SALINAS VEYZAGA, Ph.D.

leynasud@gmail.com

Ingeniería Informática

Universidad Nacional "Siglo XX"

Llallagua, Bolivia

RESUMEN

La investigación propone un modelo predictivo basado en técnicas de Big Data para identificar delitos de acoso en Facebook. Este modelo utiliza datos extraídos de comentarios en publicaciones, aplicando algoritmos de aprendizaje automático para detectar patrones de acoso, como insultos o agresiones verbales.

El estudio aborda la creciente problemática del ciberacoso, facilitado por el aumento del uso de redes sociales y dispositivos tecnológicos. Para ello, se empleó el software Facepager para recolectar datos, técnicas de preprocesamiento como limpieza de texto y tokenización, y un modelo Naive Bayes para clasificar los comentarios como acoso, no acoso o neutros.

El proceso incluyó la clasificación manual de comentarios durante cuatro meses y validaciones con profesionales, logrando un modelo efectivo que podría ser implementado en otras redes sociales.

1. INTRODUCCIÓN

Las redes sociales en Internet posibilitan la interacción con otras personas, aunque no las conozcamos físicamente, ya que la comunicación abarca geográficamente lugares cercanos y alejados. El sistema de comunicación es abierto y una persona puede colocar la información que considere conveniente, pero el acceso a esa información se habilita para todos los amigos que el usuario haya seleccionado, negando la privacidad de cierto tipo de información.

La presente investigación propone un modelo predictivo que utiliza técnicas de Big Data. Estas se enmarcan dentro de los procesos que comprenden la recolección, depuración, tratamiento, modelado y estudio de datos encaminados a la obtención de conclusiones útiles; en este caso, será para identificar delitos de acoso en la red social Facebook.

Este modelo toma como dataset información extraída de los comentarios de publicaciones en Facebook, para utilizar un algoritmo de Machine Learning. Como resultado del entrenamiento, se obtiene un modelo de predicción que pueda identificar patrones de acoso y no acoso. Estos patrones se manifiestan en agresión verbal grave, como insultos, ataques racistas, homofóbicos, entre otros. Este modelo puede ser utilizado para identificar ataques futuros en publicaciones, ya que se evidenció que los comentarios realizados en estas tienen un impacto grande en las personas, con desenlaces negativos como depresión, ansiedad y, en algunos casos, suicidio.

En un informe presentado por la Comisión Económica para América Latina y el Caribe (CEPAL, 2018), se indica que la difusión de las tecnologías digitales ha permitido un incremento exponencial de los usuarios en Internet. En 2015, se estimó que 3.174 millones de personas usaron Internet, lo que equivale al 43,4% de la población. Se prevé que esta actividad se incremente en un 60%.

Peña Castañeda (2016) relata que, en entrevista con *EL TIEMPO*, Alberto Samuel Yohai, presidente de la Cámara Colombiana de Informática y Telecomunicaciones, dijo que para los criminales ahora es mucho más sencillo actuar de manera digital que presencial.

El acoso mediante redes sociales tiene un carácter innovador y pretende disminuir los delitos a través de estas plataformas. Además, los avances tecnológicos han cambiado la forma de pensar de niños y jóvenes, quienes creen que todo lo publicado es confiable, ignorando que los delincuentes utilizan estas redes como medio para obtener sus presas.

El acoso puede ocurrir en persona y a través de la tecnología. La agresión electrónica o “ciberacoso” ocurre mediante dispositivos tecnológicos y mecanismos como correo electrónico, mensajes instantáneos, sitios web, mensajes de texto, redes sociales y aplicaciones.

Por ello, surge la necesidad de identificar patrones de conducta con tendencia a cometer acoso por medio de Big Data, de tal forma que se pueda prevenir cualquier delito que puedan sufrir los usuarios en Facebook.

Planteamiento del Problema

Diseñar un modelo predictivo para identificar delitos de acoso en la red social Facebook aplicando Big Data.

Objetivo General

Desarrollar un modelo predictivo que permita identificar delitos de acoso en la red social Facebook mediante técnicas de Big Data.

Objetivos Específicos

1. Determinar el conjunto de datos a través de la extracción de datos en Facebook, enfocados en los comentarios de publicaciones.
2. Implementar técnicas de Big Data para la identificación de patrones de comportamiento dirigidos al acoso.
3. Entrenar un modelo de aprendizaje automático utilizando los datos extraídos para identificar patrones de acoso mediante técnicas de clasificación.
4. Realizar el análisis de los resultados que presenta el modelo en el proceso de clasificación en Facebook.

¿Qué es Big Data?

Big Data se refiere a conjuntos de datos extremadamente grandes y complejos que no pueden ser analizados fácilmente con herramientas tradicionales debido a su tamaño, velocidad o variedad.

Estos conjuntos de datos suelen proceder de diversas fuentes como redes sociales, sensores, aplicaciones móviles y transacciones en línea. Las plataformas de redes sociales, como Facebook, Twitter, Instagram y TikTok, han proporcionado mecanismos de comunicación y han fomentado la creación de comunidades en línea.

Marco Teórico y Conceptual

Ciberacoso
El acoso en las redes sociales se denomina ciberacoso. Según la OPS (Organización Panamericana de la Salud), la violencia consiste en el uso deliberado de la fuerza física o el poder, ya sea en forma de amenaza o de manera efectiva, contra uno mismo u otras personas, causando daños físicos, psicológicos o incluso la muerte (Krug, Mercy & Lozano, 2003).

Ley N.º 164
Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.

Ley 243
Ley Contra el Acoso y Violencia Política Hacia las Mujeres.

Proyecto de Ley
Regula y sanciona el uso indebido de redes sociales en el Estado Plurinacional de Bolivia.

2. MATERIALES Y MÉTODOS

Extracción de Datos
Se utilizó el software Facepager para recolectar comentarios de publicaciones en Facebook.

Preprocesamiento de Datos
Incluye técnicas como limpieza de texto, tokenización, eliminación de caracteres especiales y palabras vacías (stopwords).

Entrenamiento del Modelo
Se usó Naive Bayes, dividiendo los datos en un 75% para entrenamiento y un 25% para pruebas.

3. RESULTADOS Y CONCLUSIONES

1. Los datos extraídos de Facebook fueron fundamentales para el etiquetado y preparación del modelo predictivo.
2. El proceso de clasificación manual de comentarios llevó 4 meses, verificando cada texto para entrenar el modelo.
3. Los resultados indican que el modelo es efectivo para detectar patrones de comportamiento de acoso en Facebook.
4. La encuesta realizada a profesionales permitió incorporar términos adicionales al dataset, validando así el modelo.

Recomendaciones

1. Incluir más palabras clave en el dataset para mejorar la precisión del modelo.
2. Implementar el modelo en otras redes sociales como Twitter e Instagram.
3. Usar el modelo en complementos de Facebook para eliminar mensajes de acoso, creando un entorno más seguro.
4. Comparar el modelo con otras técnicas de inteligencia artificial para obtener mejores perspectivas.

SOBRE EL AUTOR

Ingeniero informático.

Docente de la carrera Ing. Informática desde la gestión 2008.

Maestría en Ciencias de la Computación(Mención Seguridad Informática)

Diplomado en Educación superior.

Diplomado en formación basada en competencias

Diplomado en Metodología de la investigación.

Diplomado en gestión de Seguridad y Auditoría Informática.

Diplomado en Herramientas Tecnológicas para educación Superior Virtual

Diplomado en Internet de las cosas y la industria 4.0

Certificación Oficial MikroTik Network Associate.

Secretaria Ejecutiva de la FUD gestión 2015-2017

Juez en la competencia de programación ACM de la carrera Ing. informática.

Figura 1: Fotografía de presentación de la ponencia