Algoritmos contra el fraude y el crimen organizado

Investigadores de la Universidad Politécnica de Madrid han aplicado métodos matemáticos para identificar en las redes sociales a posibles terroristas y defraudadores. Los algoritmos desarrollados son especialmente útiles para detectar el fraude del IVA.

SINC 16/5/2017 11:51 CEST

Los algoritmos de inteligencia artificial, sobre todo de análisis de redes, tienen un enorme potencial en la detección de tramas de fraude y de crimen organizado. / UPM

Los algoritmos de inteligencia artificial y particularmente de análisis de redes tienen un enorme potencial en la detección de tramas de fraude y de crimen organizado. Por ello, un equipo de investigadores del departamento de Inteligencia Artificial y del Grupo de Análisis y Decisiones y Estadística de la ETSI Informáticos de la Universidad Politécnica de Madrid (UPM) ha desarrollado varios algoritmos que pueden ser utilizados para la detección del fraude y el crimen organizado a través de las redes sociales.

La proliferación de atentados terroristas y de organizaciones criminales de todo tipo ha hecho necesarias investigaciones sobre las relaciones de diferentes colectivos de delincuentes. Los métodos matemáticos y computacionales y el análisis de redes se han convertido en una herramienta fundamental en este campo.

Se han creado algoritmos y funciones que se pueden aplicar en las redes sociales para identificar a posibles defraudadores o incluso terroristas

Como ejemplo, una de las principales medidas antiterroristas impuestas tras los atentados de Nueva York, Madrid y Londres, en la primera década de los años 2000, consistió en archivar los registros de llamadas telefónicas y correos electrónicos. Los servicios de inteligencia, así como los ministerios de defensa e interior de la mayoría de los estados europeos guardan registros de terroristas junto con sus relaciones internas y externas cuyo análisis, mediante algoritmos matemáticos, marca la agenda de la lucha antiterrorista y la seguridad nacional.

De la misma manera, los organismos encargados de la recaudación de impuestos de la mayoría de los Estados poseen registros de contribuyentes y de sus conexiones a través de lazos de todo tipo (familiares, societarios, comerciales,...). Todo ello puede analizarse con objeto de detectar tramas de fraude y contribuyentes defraudadores, del mismo modo que las agencias de seguros guardan documentación de atestados y de implicados en accidentes de tráfico para buscar patrones fraudulentos entre sus clientes. No en vano, solamente el fraude del IVA causa unos perjuicios a la Unión Europea de 170.000 millones de euros al año.

En todos estos ámbitos el análisis de redes es una herramienta fundamental que, hasta hace relativamente poco, se limitaba a pequeños grafos generalmente representables visualmente.

Detectar patrones en redes sociales

“La tecnología disponible hasta hace menos de una década, así como la inexistencia de mecanismos eficientes de generación y almacenamiento de grandes redes, imposibilitaba el análisis masivo de redes”, explica Alfonso Mateos, uno de los investigadores UPM que ha participado en el estudio. “Sin embargo, en la actualidad, las tecnologías permiten establecer nuevos planteamientos que implican la creación de algoritmos capaces de detectar

en las redes sociales y de comunicaciones ciertos patrones que identifican a criminales y defraudadores", añade.

> Los comportamientos de los criminales y defraudadores se parecen entre sí y se pueden distinguir del de las personas honradas

¿En qué se basan los algoritmos para detectar a un sospechoso?. "Los criminales y defraudadores se parecen entre sí y sus comportamientos son similares", explica Alfonso Mateos. Partiendo de esa base, se puede identificar un grupo de variables individuales de las personas y empresas cuyos valores pueden servir para distinguir sus comportamientos de aquellos realizados por las personas honestas y honradas y las empresas que dirigen. Es ahí donde entran en juego varios algoritmos de Aprendizaje Automático y Estadística Multivariante que permiten definir las variables a las que hay que prestar atención.

Por otro lado, indican los expertos, "los criminales o defraudadores cooperan entre sí (como sucede en la creación de empresas carrusel en el IVA) y aprenden unos de otros y de los profesionales que les asesoran". Según esta hipótesis deben existir ciertas relaciones entre patrones de defraudación que permiten el empleo de algoritmos de análisis de redes y teoría de grafos para encontrar tramas, intermediarios y actores en la sombra.

En base a todos estos criterios, los investigadores han creado varios algoritmos y funciones que se pueden aplicar en las redes sociales para identificar a posibles defraudadores o incluso terroristas. "Desde la lucha antiterrorista hasta el blanqueo de capitales los algoritmos que hemos desarrollado nos pueden dar pistas de que algo no va bien y ayudarnos a encontrar a los que están cometiendo un delito".

No es extraño, por ello, que ya hayan sido varios los organismos internacionales que han mostrado interés en este proyecto en el que también colabora el Ministerio de Economía, Industria y Competitividad y funcionarios de la Agencia Tributaria en el ejercicio de sus competencias: "En el ámbito tributario la OCDE y la IOTA han situado el empleo de este tipo de funciones

y algoritmos entre sus prioridades y convocado reuniones multilaterales durante este año en Dublín y Budapest", explican los autores, que publican su trabajo en la revista *Modeling Decisions for Artificial Intelligence.*

Referencia bibliográfica:

Vicente, E., Mateos, A. Jiménez-Martín, A. (2016). "Complicity Functions for Detecting Organized Crime Rings, Modeling Decision for Artificial Intelligence". V. Torra, Y. Narukawa, G. Navarro-Arribas, Cr. Yañez (Eds.). *Modeling Decisions for Artificial Intelligence*, 2016.

TAGS | CIBERTECNOLOGÍA | FRAUDE | INTELIGENCIA ARTIFICIAL | TECNOLOGÍA