El País 16/05/2020

LA LUCHA CONTRA EL CORONAVIRUS

La Universidad Autónoma de Madrid se alía con los marines de EE UU para combatir los bulos sobre la covid-19

La forma que cada uno tenemos a la hora de teclear permite al sistema TypeNet identificar con gran precisión múltiples cuentas gestionadas por un mismo usuario

Montaje de un teclado de ordenador con la palabra 'fake news' ('bulos')DIMARIK / GETTY IMAGES/ISTOCKPHOTO

El País 16/05/2020

GUILLERMO VEGA

La premisa es clara: desarrollar máquinas que sean capaces de verificar la identidad de una persona a partir de la forma en la que teclea en su ordenador y evitar que propaguen bulos sobre la covid-19. Y ello, con menos de 15 palabras. Este sistema biométrico de identificación se denomina *dinámica de tecleo*, y es la base de TypeNet, un proyecto conjunto del Biometrics and Data Pattern Analytics Lab de la Universidad Autónoma de Madrid (UAM) y un laboratorio de investigación de la Naval Postgraduate School de la marina estadounidense (US Navy). Este programa persigue crear algoritmos que ayuden a identificar a usuarios detectados como propagadores de noticias falsas o desinformación.

Cada uno tenemos características propias a la hora de escribir: por ejemplo, lo que dura la presión de las teclas y lo que tardamos en pulsar la siguiente. Los navegadores con los que accedemos diariamente a

Internet están preparados para recoger esa información. Esta técnica biométrica lleva, de hecho, bastante tiempo entre nosotros: durante la Segunda Guerra Mundial, los servicios de inteligencia militar identificaban a distintos individuos por su forma de enviar mensajes en código morse. “Las primeras contribuciones científicas son de hace varias décadas”, explica Javier Ortega García, catedrático de Teoría de la Señal y Comunicaciones y director, Biometrics & Data Pattern Analytics Lab en la UAM (institución de la que, además, es vicerrector). “Pero hasta hace pocos años no ha habido suficiente capacidad tecnológica y avances en *deep learning* para que pueda formar parte de un sistema comercial.

A esta tecnología se le puede dar muchos usos. Uno de ellos, frenar la propagación de bulos (*fake news*) gracias a TypeNet, el sistema de identificación biométrica que en un futuro puede permitir bloquear a

internautas y cuentas dedicadas a la propagación de noticias falsas. “Estos usuarios se amparan en el anonimato y en la deslocalización de internet para propagar la desinformación y el miedo sobre la pandemia de coronavirus”, explica Aythami Morales, investigador y profesor de la UAM y coordinador de este trabajo, en el que, además, han participado Alejandro Acien, Julián Fierrez, Rubén Tolosana, Rubén Vera-Rodríguez, John V. Monaco y Yurena López. Su trabajo será presentado en julio en una conferencia sobre Seguridad organizada por la asociación internacional IEEE.

Estos investigadores llevan dos meses trabajando en adaptar esta tecnología a la lucha contra la desinformación relacionada con la covid-19. ¿Cómo? TypeNet, en primer lugar, extrae los patrones asociados a la forma de teclear de cada persona, independientemente del texto que teclee. Después, el

sistema elabora un algoritmo que permite modelar fielmente a cada individuo a través de patrones neuromotores asociados a su forma de teclear.

Con este procedimiento se logra un modelo de identificación que permitirá bloquear a usuarios y cuentas dedicadas a la propagación de noticias falsas. “Plataformas como Twitter o Facebook tienen problemas para luchar contra la propagación de estas noticias ya que una vez detectan y cancelan una cuenta dedicada a desinformar, sus creadores tardan pocos minutos en crear otra”. asegura Artiles.

Así, el modelo de la UAM y de la Naval Postgraduate School (creado a partir de cuatro millones de muestras de 160.000 internautas; cinco gigas de información en total) permitirá usar los datos biométricos sobre dinámicas de tecleo para identificar múltiples cuentas gestionadas por un mismo usuario. Una vez ese usuario

es expulsado por difundir bulos, el sistema lo identificará aunque genere una nueva cuenta basada en una identidad falsa. “Las pruebas realizadas sobre más 100.000 cuentas muestran cómo es posible identificar cuentas anónimas con porcentajes que llegan alcanzar el 50% de precisión”, sostiene Morales. “Esto se traduce en más de 50.000 cuentas *desanonimizadas* a través de esta tecnología”.

EL ORIGEN DE LA COLABORACIÓN

La colaboración de la UAM y la marina estadounidense se inició en septiembre de 2019, cuando un estudiante de Doctorado de la UAM, Alejandro Acién, se trasladó a Monterrey para levar a cabo una estancia de investigación de tres meses bajo la supervisión del investigador y referente mundial en el campo Vincent Monaco. Durante su estancia, se estudiaron nuevos algoritmos de aprendizaje profundo

('deep learning') capaces de modelar la dinámica de tecleo, explica Aythami Artiles

Privacidad

Aythami Morales admite que el gran potencial de esta tecnología puede tener usos no tan beneficiosos: “Si caen en las manos incorrectas, estas tecnologías se podrían usar para perseguir a usuarios por sus ideas políticas y coartar la libertad de expresión”, avisa. “Un gran poder conlleva una gran responsabilidad”, concluye citando a Franklin D. Roosevelt (y a Peter Parker, claro está). “Las leyes de proyección de datos ponen los frenos necesarios, y en todo momento hay que cumplir los requisitos de la normativa”, concluye. Entre ellos, que se manejen datos anónimos, que terceros no tengan acceso a ellos, que los usuarios estén informados y que exista un tiempo limitado de almacenamiento.

Otros usos

La dinámica de tecleo puede constituir una herramienta poderosa para muchos ámbitos. “No es la biometría más difundida, pero aun así resulta muy típico encontrarlo en todos los procesos online. Siempe que haya un usuario en un dispositivo a cualquier tipo de servicio es susceptible para aplicarlo”, asegura Javier Ortega García.

El primero uso de la *biometría conductual* que viene a la cabeza es el de la seguridad informática y la identificación. “Con la crisis sanitaria provocada por el cornavirus se ha puesto de manifiesto la necesidad de la enseñanza online: tenemos que implantar la docencia telemática y hay que evaluar remotamente a estos alumnos. La dinámica de tecleo supone una forma de asegurar que se trata en realidad de un estudiante determinado o de que no está aplicando prácticas dudosas”. Y tiene otra ventaja: esta herramienta

permite una monitorización continua de la identidad. Plataformas como Coursera, asegura Ortega, ya cuentan con herramientas de este tipo.

La forma en que escribimos en nuestros dispositivos también puede tener usos en la medicina. La propia UAM lanzó el pasado año un programa llamado BioGuard que tiene en cuenta la forma en la que un usuario sujeta el terminal, presiona la pantalla, teclea, hace *scroll* o *swipe*, agranda una imagen con los dedos, arrastra un icono o hace una búsqueda por voz. A través de aprendizaje automático y las redes neuronales profundas propias del *deep learning* extraemos este tipo de información biométrica para conocer con mayor profundidad al usuario, y con un tratamiento correcto de esta información podría aplicarse en el mundo de la medicina para que móviles y tabletas ayuden a identificar algunos estadios o etapas iniciales de

enfermedades neuromotoras o neurodegenerativas como párkinson o alzhéimer.

PROBLEMA

La profusión de bulos lleva años constityendo un grave problema social. Con el estallido de la pandemia, sin embargo, ste ha alcanzado cotas peligrosas. Esta semana, más de un centenar de profesionales de la medicina y de la enfermería de 17 países han enviado una carta a los responsables de Facebook, Twitter, Google y YouTube en la que alertan del impacto sobre la salud de los bulos y la desinformación sobre la covid-19. Varios premios Nobel, reunidos en la Comisión Internacional para la Información y la Democracia, han hecho recientemente un llamamiento a las plataformas digitales para que luchen eficazmente contra las noticias falsas.