NOTA DE ACTUALIDAD 8/2018
23 de abril de 2018

Laura Orallo *

¿Qué son los Bots?

Nota de actualidad 8: ¿Qué son los Bots?

Un "bot" es un software diseñado con funcionalidad para interactuar y comunicarse con el usuario imitando su comportamiento. Los bots son asistentes de ordenador. Estos programas se encuentran en aplicaciones con la función de ayudar a los usuarios.

La palabra ha tomado varios significados en función del uso que se les dé. Pueden ser utilizados para la reserva online de vuelos, hoteles, comida a domicilio, etc. Pero también aparecen de manera frecuente en redes sociales como Facebook, Twitter y Skype. En el mundo de los videojuegos, en cambio, los programadores utilizan los bots como Inteligencia Artificial en los juegos. Algunos bots tienen una inteligencia artificial más sofisticada y tratan de imitar el lenguaje humano en toda su complejidad, llegando a mantener conversaciones.

La mayoría, solo ejecutan una serie predeterminada de conceptos relacionados con su función: comprar sushi, reservar una casa rural, pagar un recibo o poner música. Pero en la actualidad se conocen por su papel en ciberdelitos, en forma de ataques de spam en emails o incluso para derribar páginas web y colapsar sistemas oficiales.

La parte 'revolucionaria' es que estos bots no necesitan nada especial para ejecutar sus acciones, no requieren conocer una herramienta o aprender un lenguaje por parte del usuario: basta decirles lo que quieres y ellos lo interpretan y lo hacen.

La Historia de los Bots

En contra de la idea de que los bots son algo novedoso, es necesario remontarnos a 1966 cuando Joseph Weizenbaum programó el primer "bot" llamado Eliza. El programa simulaba a un terapeuta con el cual se podía "hablar" mediante preguntas, las cuales eran contestadas como si fuera un terapeuta con "¿cómo te hace sentir eso?"

* Alumna en prácticas del Master de RRII de la Universidad de San Pablo CEU

Las opiniones contenidas en las notas CAP son responsabilidad de sus autores, sin que reflejen necesariamente el sentir de la Guardia Civil

Más adelante llegaría el buscador de Google, la herramienta de Internet más usada de la historia. Y su éxito viene de su simplicidad: tecleas lo que quieres buscar y Google lo busca por ti.

Otro caso curioso ha sido Anna, una asistente virtual creada en 2006 por Ikea para ayudar a los clientes a localizar lo que deseaban en la tienda, basándose en una serie de respuestas. "Pídeles lo que quieras, como quieras y ellos te entenderán"[1].

También hay que recordar que en 2010 Apple lanzó el iPhone 4s con una novedad, Siri, un bot con personalidad. Dos años después Google puso en marcha Google Now y en 2014 Microsoft lanzó Cortana. Los tres bots interaccionan por medio de la voz y pueden hacer búsquedas en internet, pedir un taxi o abrir aplicaciones solo con una instrucción de voz. Estos bots se consideran de nueva generación por su elemento de Inteligencia Artificial asociado a ellos.

La transcendencia de los Bots en la actualidad

En la actualidad se han convertido en interés popular por el impacto en las redes sociales como Twitter. Los bots se están programando para lanzar tuits automáticamente y sistemáticamente al flujo de la red social. La complejidad se encuentra en que en ocasiones los tuits se lanzan de cuentas con nombres y perfiles similares a los reales, por lo que se complica la detección. Las alarmas saltan con el número y frecuencia de publicaciones, siendo más elevada que la media y levantando así las sospechas que incitan al análisis de la cuenta.

El acontecimiento que más de cerca vivimos involucrados se refiere a los tuits difundidos automáticamente respecto al proceso independentista de Cataluña. Según fuentes de Audiese, unos 4.883 perfiles de Twitter difundieron automática y sistemáticamente mensajes sobre el proceso independentista de Cataluña, supuestamente financiados por el gobierno ruso. Se estima que desde el 29 de septiembre al 19 de octubre se compartieron más de 84.000 mensajes en Twitter por unas 38.000 cuentas con enlaces o contenidos de RT o Sputnik, todas ellas hablaban de Cataluña. 13 de cada 100 cuentas se encontraban asociadas a la cadena televisiva RT (Russia Today), propiedad del gobierno ruso, y a Sputnik, agencia, portal web y radio de la agencia de noticias Rosilla Segodnya, también controlada por el gobierno ruso[2]. Ante la continua involucración de estas cuentas en la

[1]http://www.revistagq.com/noticias/tecnologia/articulos/que-son-exactamente-los-bots-y-como-funcionan/25633
[2]https://politica.elpais.com/politica/2017/12/04/actualidad/1512389091_690459.html?rel=str_articulo#1519204786798

difusión de campañas propagandísticas maliciosas, Twitter decidió restringir la parte de difusión de ambas agencias, RT y Sputnik y anunció que no emitirá más publicidad.

El mayor escándalo saltó en 2016 durante las elecciones para la presidencia norteamericana con la difusión de noticias falsas no solo en contra de Hillary Clinton y apoyo a Trump, sino en la difusión de informaciones para desfavorecer a otros candidatos y crear un ambiente de descontento, pro-manifestaciones y desmovilización de minorías. El fiscal especial Robert Mueller, encargado de llevar la trama rusa, ha destapado la estrategia de Rusia y su armamento de "fake news" acusando a 13 ciudadanos rusos y tres empresas rusas de elaborar esta trama (Internet Search Agency LLC, Concord Management and Consulting y Concord Catering), nombrada Proyecto Laktha, contra las elecciones americanas en 2016. Según Mueller, es una "guerra de información encaminada a generar desconfianza hacia los candidatos y el sistema político en general"[3].

La campaña en la carrera de Trump para presidir la Casa Blanca sirvió como patrón para lo que acontecerá en las campañas presidenciales en Europa a favor del Brexit, en Francia apoyando a Marie LePen sobre Macron, con la ultraderecha alemana y holandesa; en todos los casos se crearon perfiles falsos, surgieron bots, aumento de "fake news", técnicas para crear la confusión mediante anuncios pagados, astroturfing y otras herramientas. La teoría detrás de estas campañas sería la estrategia del Kremlin para consolidar su presencia internacionalmente mediante la promoción de las fracturas europeas, debilitando así el frente europeo. El caso más reciente en EE.UU. ha sido apoyando las campañas en contra de las armas y movimiento de control más sistemático de las mismas, tras los tiroteos de Florida en febrero de 2018[4].

Desde EE.UU. no ven productivos los intentos del Kremlin de polarizar a la sociedad con su apoyo a las extremas derechas e izquierdas, afirmó el teniente general McMaster en el último congreso de seguridad. Para EE.UU. la injerencia rusa no está haciendo más que unir a la población y los distintos países que se están viendo envueltos en los ataques de Rusia[5]. Estas publicaciones no solo ocurren en Twitter; Facebook y Youtube, que no se libran de estas difusiones. Según el director ejecutivo de New Knowledge, empresa que se encarga de perseguir a los bots malignos, se encuentran en cualquier movimiento social que pueda involucrar una división en la población.

[3] https://elpais.com/internacional/2018/02/16/estados_unidos/1518805614_412828.html
[4] https://elpais.com/internacional/2018/02/20/estados_unidos/1519112012_207210.html
[5] https://elpais.com/internacional/2018/02/17/actualidad/1518893869_513174.html

La preocupación se ha trasladado a México, Brasil, Colombia e Italia, que celebran sus próximas elecciones en 2018. Tras la lección de 2016 y 2017, estas naciones se encuentran preocupadas por la posible injerencia rusa y las consecuencias que pueden acarrear para el futuro político en estos países.

Es importante resaltar que no son solo los rusos quienes están empleando esta estrategia de desinformación - "fake news". Según el informe publicado por la organización estadounidense Freedom House, fundada en 1941 y dedicada a la vigilancia independiente de la libertad de los ciudadanos, la libertad de expresión, respeto de los derechos de las minorías y las mujeres, derechos humanos y democracia en el mundo, se denuncia que alrededor de 30 países se encuentran empleando los llamados "ejércitos de formadores de opinión" para difundir opiniones, impulsar determinadas agendas y contrarrestar las críticas en las redes sociales. El número de gobiernos que han decidido controlar este flujo de información falso ha aumentado cada año desde que Freedom House comenzó a rastrear sistemáticamente el fenómeno en 2009. Aunque esta práctica, en los últimos años, se ha vuelto mucho más generalizada y más sofisticada técnicamente, con bots promulgadores de propaganda y noticias falsas explotando las redes sociales y buscando algoritmos que garanticen una alta visibilidad y una conexión factible como información de confianza[6].

Herramientas para frenar a los bots maliciosos

Pero, ¿cómo se pueden frenar estas amenazas? ¿Cómo se pueden intervenir los bots maliciosos? La detección es difícil. Twitter a la semana detecta alrededor de 50 millones de bots detrás de 3,3 millones de cuentas que pueden ser calificadas de sospechosas. Existen algoritmos de detección con una tasa de éxito de alrededor del 75%, incluso llegando al 95%. Otro elemento de análisis mecanismo que muchas plataformas están introduciendo para asegurarse que hay un ser humano detrás de las cuentas, es que no suelen establecer un diálogo con otras personas y se limitan a difundir contenidos. Para establecer controles se están aumentando los sistemas de verificación tipo reCAPTCHA o la verificación mediante un código de acceso enviado al teléfono móvil con la intención de detectar si un humano está abriendo una cuenta o si es un proceso automatizado con intenciones aviesas. Esta última medida está provocando controversia, ya que choca con el aspecto de privacidad.

[6] https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf

Plataformas como Wikipedia han elaborado una estricta política que todos los bots deben cumplir. Facebook por otro lado, estaba valorando que los usuarios suban un selfie para demostrar que no son bots.

En enero Twitter anunció que, como parte de sus esfuerzos de mantener la calidad en la información de su portal, se producirían cambios en sus herramientas TweetDeck y la API para limitar la capacidad de los usuarios para realizar acciones coordinadas en múltiples cuentas. Estos cambios supusieron un paso importante para garantizar la seguridad y mantener al margen la actividad maliciosa en historias de relevancia como unas elecciones. El pasado miércoles 21 de febrero Twitter dio un paso más para evitar la actividad maliciosa de bots, prohibiendo la automatización de los tuits desde diferentes cuentas para tratar de combatir los problemas bots, spam y manipulación[7]. No va a permitir a los usuarios que publiquen simultáneamente contenido idéntico o sustancialmente similar en varias cuentas. Tampoco permitirá realizar acciones simultáneas como "Me gusta", "Retweets" en varias cuentas. El uso de cualquier forma de automatización (incluida la programación) para publicar contenido idéntico o sustancialmente similar, o para realizar acciones como Me gusta o Retweets, en muchas cuentas que han autorizado su aplicación (ya sea que haya creado o controlado directamente esas cuentas) no está permitido. Los usuarios de TweetDeck ya no podrán seleccionar varias cuentas a través de las cuales realizar una acción como twitter, retweeting, me gusta o seguir [8].

Tras el incremento de “fake news” mediante perfiles falsos en las redes sociales, el número de herramientas para identificar estas cuentas ha ido en aumento. Mencionando algunas, Twitter Counter[9], herramienta que se encarga del recuento a los seguidores de cuentas en Twitter durante un período de tiempo. Mediante este ejercicio, la intención es buscar cualquier tipo de actividad anormal, como un aumento repentino de seguidores.

Twitter Audit es otra herramienta que analiza la lista de seguidores de un usuario, determina qué porcentaje de esos seguidores son falsos y arroja una puntuación de auditoría de entre 1% y 100%. La herramienta analiza algunos criterios para llegar a su puntuación, incluyendo el número de tuits, fecha del último tuit y la relación de los seguidores con los amigos que cada seguidor tiene.

[7] https://computerhoy.com/noticias/internet/twitter-pone-cerco-automatizacion-tuits-combatir-bots-76311
[8]https://blog.twitter.com/developer/en_us/topics/tips/2018/automation-and-the-use-of-multiple-accounts.html
[9] http://twittercounter.com/

Cualquier puntaje por encima del 60% se clasifica como "real", mientras que los puntajes de entre 40% y 60% se clasifican como "no seguro".

El Observatorio de las redes Sociales (Observatory on Social Media - OSoMe[10]), detrás la Universidad de Indiana, se encuentra desarrollando herramientas públicas para el diagnóstico de bots, cuentas falsas y ayudar a los usuarios con este problema. La web Botometer[11] permite analizar cuentas de Twitter y hacerse una idea de si se comportan como bots o como humanos. "Botometer se puede utilizar junto con otras herramientas de nuestro laboratorio para estudiar cómo los memes o los hashtags se difunden en Twitter y quién los comparte", señala Filippo Menczer, uno de los fundadores del Observatorio[12]. Otra de las herramienta que han desarrollado es Hoaxy[13], encargada de rastrear la propagación de estas "fake news" y desinformación. El proyecto es que para 2018 ambas herramientas se integren y sean una fuerte estrategia para estudiar los bots sociales en su difusión.

Este Observatorio también se encuentra realizando proyectos con terceras instituciones y alumnos de la universidad de Indiana que utilizan las APIs desarrolladas por este Observatorio para la detección de bots. Entre ellas figura "Boston"[14], que se encuentra construida sobre Botometer y se trata de una extensión de Chrome para detectar y bloquear bots en los muros de Twitter. Esta aplicación se encarga de analizar señales en el contenido e intencionalidad de los tweets, patrones de red, tiempo de actividad, etc., para crear modelos precisos para identificar bots. También nos encontramos con "Probabot"[15], perfil en Twitter, que tras las estadísticas que emite Botometer, se lleva a cabo una "caza" de bots en cuentas con actividad política.

Los bots no son un problema sencillo, ya que en la actualidad se está centrando la atención en otorgar a estos softwares informáticos un componente malévolo, pero hay que recordar que también hay bots positivos. Estos se encargan de alertar, por ejemplo, de desastres naturales, de los niveles de calidad del aire o para avisar de averías en el transporte público. También pueden ayudar a controlar la suplementación de IP en nombre de gobiernos, como en el Caso de Canadá, tuitean cada vez que alguien con una dirección IP del gobierno escribe.

[10] http://osome.iuni.iu.edu
[11] https://botometer.iuni.iu.edu/
[12] https://elpais.com/tecnologia/2017/11/30/actualidad/1511998006_098595.html?rel=str_articulo#1519204786798
[13] http://hoaxy.iuni.iu.edu/
[14] http://botson.net
[15] https://twitter.com/probabot_