BOTS Y AUTOMATIZACIÓN

Diego Cerqueira

1

BOTS PARA TODOS LOS LADOS:

LOS DESAFÍOS DE LA DETECCIÓN DE BOTS EN LAS REDES SOCIALES

Retomando la discusión sobre la influencia de la automatización y su relación con los fenómenos de desinformación, seguramente has acompañado que en las últimas semanas el debate de las CPMI de las Fake News ha sido muy acalorado. La comisión parlamentar fue construída para pesquisar no solo las redes de perfiles enfocadas en propagar noticias falsas, como también para entender quiénes son los actores que financian esas redes, visto que los objetivos ya se han aclarado: manipulación de la opinión pública. Esse tipo de pesquisa no es algo exclusivo del escenario brasileño, mucho menos algo nuevo. Desde 2016/2017, ya se pesquisaba los impactos de variados usos de las redes sociales como estratégia de influenciamiento y manipulación de la opinión pública.

Hace algunas semanas este tema salió a luz nuevamente cuando dos miembros del equipo de Twitter publicaron el artículo “Bot or not” en el blog de la plataforma, criticando algunas herramientas de detección de bots propias en la red, específicamente el Botometer y el Bot Sentinel. La idea central del artículo fue defender que ese proceso no puede ser solo “ES BOT o no BOT”. En las palabras de Yoel Roth y Nick Pickles: “necesitamos realizar análisis holísticos sobre los casos para no punir usuarios que, a pesar de presentar algunas características de “bot” son usuarios verdaderos”. Todo eso para decir que encontrar, detectar y remover los bots es un desafío, sobre todo sin cometer injusticias con usuarios que, por casualidad, quieran tener sus perfiles más autónomos o tengan un conjunto de atributos relacionados a su actividad de forma a clasificarlo como más bot que otros usuarios.

¿LOS BOTS SON TODOS IGUALES?

La respuesta técnica es sí - sus diferencias reales van por cuenta de sus usos y aplicaciones, su finalidad básicamente -, pero no es por este camino que vamos a seguir, si el bot es centinela del bien como Rosie, Beta ou M0na, vamos apenas exaltar las iniciativas.

En el primer texto de esta serie sobre automatización y desinformación, separamos bots en dos categorías: los que se esconden e intentan camuflarse de humanos y los robots asumidos, como chatbots o robots asistentes en tu móvil. Dicho esto, lo que haremos ahora es añadir una pequeña camada de complejidad dentro de la primera categoría, al crear una subcategoría, que separa los bots de lo que llamamos trollbots.

ABECEDARIO DEL ARTÍCULO

¿QUÉ SON LOS TROLLBOTS?

El término trollbot deriva del internetés troll, aquél que “trollea” alguien, en inglés trolling. Un troll puede ser su sobrino o sobrina adolescente que vive compartiendo imágenes con bromas, textos que bloquean el ordenador de otros - hay extremos - los que desde dentro de la comodidad de sus hogares, escondidos detrás de una pantalla y hace algunas centenas de kilómetros de distancia, actúan sin pensar en las consecuencias, atacando, distribuyendo odio gratuito por medio de comentarios y publicaciones ofensivas en foros, sitios y redes sociales.

De esta manera, los trollbots son un tipo de bot que actúan en las redes sociales y, diferente de los bots tradicionales, son especialistas en realizar ataques coordinados a determinados sitios o perfiles. Sí, los trollbots actúan como un ejército para ofender o destruir la imagen de alguien.

¿CUÁLES SON LAS DIFERENCIAS DE LOS BOTS TRADICIONALES?

Pensando en los bots, su principal diferencia es el comportamiento que cada uno de ellos ejerce en las redes. Pensando en los bots y trollbots, algo que está presente en ambos casos es la automatización, que explicaré nuevamente abajo.

¿AUTOMATIZACIÓN?

Automatización es tornar una tarea, antes realizada de forma manual por un humano (ojalá), en una tarea repetible y realizada por una máquina - en el caso de los bots, un ordenador. Esta automatización es común y, desde que creamos el ordenador (PC) que conocemos, ella es responsable de transformar el modo como realizamos diversas acciones, una vez que, de manera simple podríamos definir el ordenador como una grande calculadora, capaz de realizar tareas repetitivas en la velocidad que ningún humano es capaz.

AUTOMATIZACIÓN: ¿LA GRAN VILANA?

No. Y no podemos ser reducionistas aquí. El uso de máquinas para la realización de tareas repetitivas posibilitó a los seres humanos más tiempo libre para el pensamiento creativo y, consecuentemente, para las innovaciones. Al contrario de los ordenadores, nuestro cerebro suele ser pésimo en acciones monótonas y repetitivas, ya que nos distraemos con frecuencia (algunos más, otros menos), pero excelente para romper los patrones y crear algo nuevo.

PASMEN: aún cuando hablamos de automatización en las redes sociales, ni todas son malas o prohibidas dentro de determinados límites. Esas reglas varían de plataforma a plataforma.

Las grandes problemáticas sobre el uso de la automatización son las dos: 1) Ataques coordinados y 2) viralización de contenido. Hablaremos un poco sobre cada un de los escenarios.

1. ATAQUES COORDINADOS:

Los ataques coordinados, también conocidos como linchamientos virtuales, infelizmente es un fenómeno común en las redes. Normalmente, está direccionado a figuras públicas, cuando sus opiniones divergen de algún pensamiento o posicionamiento ideológico más extremado. ¿Problemas? Diversos, principalmente relacionados a la libertad de expresión, una vez que el objetivo de estos ataques es destruir la imagen pública de un individuo o institución, desacreditar y silenciar opiniones. Hay casos en que el autor es “forzado” a remover el contenido o desactivar su perfil en la red social para dejar de sufrir ataques, una forma clara de promover censura en la red. Por supuesto que ni todos los linchamientos virtuales son promovidos por bots o trollbots, ya que este tipo de acción puede ser coordinada por grupos ideológicos en efecto manada, mezclando cuentas falsas gerenciadas por humanos, perfiles personales y también robots.

2. VIRALIZACIÓN DE CONTENIDO:

Esa es la actuación más clásica de los robots y su objetivo principal es falsificar el “viral” en las redes como un comportamiento orgánico. Un viral en internet es un contenido que está en la “boca” de todo el mundo, capaz de crear los grandes fenómenos de internet y revelar talentos. El sueño de todo creador de contenido digital, ¿verdad?

Un viral es una ola que está relacionada a un gran número de usuarios interesados, comentando y compartiendo el mismo tema. ¿Y cuál es el interés de los robots? Manipular este comportamiento. Una vez que vivimos en una sociedad mediada por algoritmos y

sistemas de tendencia, recomendación y burbujas de interés, los bots buscan influenciar dentro de una red de robots para tornar determinados contenidos virales entre sí. El objetivo es que el contenido transborde su red (botnet), una vez que sus "cebos" son enganchados por los algoritmos de las redes sociales. ¿El resultado? El contenido empezará a ser recomendado para otros usuarios reales que posiblemente puedan tener interés en el tema o no, ultrapasando una malla de robots.

LOS DESAFÍOS SON VARIADOS

MÁS QUE IDENTIFICAR EL ROBOT, NECESITAMOS IDENTIFICAR QUIÉN NO LO ES

Dentro de los desafíos enumerados en la parte uno del texto, decidí profundizar un poco más sobre el tema, pensando en cómo tornar más explícito y lo cuán complicado puede ser identificar los bots en las redes sociales. Inicialmente una detección de bot empieza con la premisa ", ¿qué es considerado normal?. Dibujando una línea entre normal y anormal, prácticas más comunes cuantifican el comportamiento en variables (¿te acuerdas de las características enumeradas en el primer texto?) sobre su público objetivo/usuarios, creando un perfil de comportamiento. Una vez que entiendas qué es un humano, por ejemplo, sabrás decir lo que no es, ¿verdad? Podría ser, pero no debería. Si pensamos de esta manera, podemos crear una máquina de injusticia, uno de los desafíos que presento en la próxima sección.

LA MÁQUINA DE PUNICIÓN ALGORÍTMICA

El objetivo normalmente es identificar bots y removerlos, pero no es tan simple. Empezando por posibles puniciones a usuarios con características y comportamientos semejantes a los "bots', o un outlier, que se asemejan a las características de robot, mencionadas en el primer texto. Un ejemplo: Piensa en el usuario super activo en Twitter, una celebridad o influenciador digital en contraposición a mi madre utilizando el Twitter. Las actividades (tiempo conectado, publicaciones, me gusta, etc) de una celebridad son diferentes y superiores a la media de los usuarios.

Complejidades son añadidas cuando existe el uso de herramienta de automatización, sea para publicación agendada o cuando hay más de una persona utilizando una misma cuenta, por ejemplo una organización. No hay como meter todo mundo en mismo "saco" y punir un influenciador por ser muy activo o mi madre por solo compartir publicaciones y no escribir nada con sus propias palabras.

¿Una solución? Apostar en la educación digital me parece una excelente alternativa. Mejor que entregar un diagnóstico taxativo sobre ser o no ser bot, es muñir el usuario de herramientas y capacidad para cuestionar los fenómenos a su alrededor. Este me parece el camino más adecuado y asertivo para la construcción de una sociedad más consciente y menos susceptible a las manipulaciones.

Se llegaste hasta aquí, te invito a conocer mi canal en Youtube llamado Desenrolando. Allí creo contenidos para diseminar conocimiento sobre los temas relacionados a internet y sus impactos en la sociedad. Está ocurriendo una serie de videos sobre Automatización, Bots y Fake News. Como suelen decir en el universo youtuber, ¡dale like y suscríbete al canal!

¡ABRAZOS Y HASTA EL PRÓXIMO TEXTO O VIDEO!