INTRODUCCIÓN AL CONCEPTO DE BOTS

Diego Cerqueira

1

YO VEO ROBOTS Y ELLOS ESTÁN POR TODA PARTE:

(CASI) TODO LO QUE NECESITAS SABER SOBRE BOTS Y METODOLOGÍA PARA LA DETECCIÓN DE AUTOMATIZACIÓN

Con la batalla de narrativas en las redes, “fake news” y “robots” se han convertido en expresiones que están en la punta de la lengua de los usuarios de las redes sociales. El escenario del ringue virtual no es exclusividad de Brasil, pero, una vez que somos un pueblo acogedor (¿verdad?), el termino bot, derivado del inglés robot, ha llegado para quedarse y ya posee una galería propia de memes: “¡es bot! - gritamos por toda parte. Claro que siempre necesitamos recordar que el uso de los bots en las redes sociales no es algo nuevo, visto que siempre han estado entre nosotros, pero de manera poco relevante, dejados de lado. Fue a partir de la consolidación de la internet como plataformas de comunicación y verdaderos palcos políticos que el tema ha ganado más popularidad y relevancia – ya que el mercado de las automatizaciones de perfiles también ha crecido bastante, ¿verdad?

Tras el 2016, algunas cosas ya han quedado claras: tuvimos un gran cambio en los intermedios de la información y la internet pasó a tener un enorme poder en la construcción de discursos y sus legitimaciones ante la opinión pública, puesto que nunca imaginaríamos que 280 caracteres podrían destruir relaciones diplomáticas. Es en este mundo que los bots están insertados para hacer que los mensajes transiten en las redes, haciendo valer el buen internetés: “si está en internet es verdad”. Sus objetivos pueden ser diversos. Pues, si hay bot para todo, lo que nos interesa en este artículo es hablar de aquellos que son utilizados para conquistar y manipular la opinión pública por medio de acciones coordinadas; o sea, bots utilizados para visualizar informaciones, descreer adversarios y dificultar el debate político.

En este artículo vamos a explorar diversos aspectos sobre el uso de robts en las redes, definir conceptos importantes, explorar herramientas de educación mediática como el Atrapabot[1] y hablar sobre los principales desafíos para la detección de bots.

¿Tienes mucho trabajo? ¡Imagínate quiénes chequean las fake news! Reproducción: Agência Lupa

DEFINICIONES BÁSICAS QUE NECESITAS SABER

1. ¿QUÉ ES UN ROBOT (BOT)?

Bot es un programa de ordenador o un script que contiene un conjunto de instrucciones (o tarea) que operan para realizar algún tipo de automatización. Ordenadores son muy buenos en realizar tareas repetitivas, considerando que no se aburren y son mucho más rápidos que nosotros, humanos. Una cosa que llevamos segundos para realizar, un robot hará en fracciones de segundos. Es importante resaltar que ni todo programa de ordenador es un bot, a pesar de que todo bot es un programa de ordenador.

Spoiler: Ellos están por toda parte.

2. COMPORTAMIENTO DE BOT O BOT-LIKE BEHAVIOR

Ahora que ya sabes que es un bot, el segundo paso es definir lo que es "comportamiento de bot" o bot-like bhavior, uno de los conceptos más importantes en esta aventura de caza a los soldados de la desinformación.

Hay dos tipos centrales de robots: primero, aquellos que no muestran la cara y hacen de todo para pasarse por humano, sobre todo en las redes sociales. El segundo tipo es el de los "robots asumidos", como las robts Rosie (desarrollada por la Operação Serenata de Amor, proyecto de la Open Knowledge Brasil) y Beta (desarrollada por el Nossas), que utilizan las capacidades de automatización para fines cívicos. Los bots de los cuales trataremos son los que buscan imitar el comportamiento humano. ¿Estás listo?

3. ¿POR QUÉ EL TWITTER?

Sabemos que el twitter no es la red social más popular entre los braisleños, pero es el favorito de los investigadores y entusiastas de los estudios de medias sociales, automatización y ciencia de datos. ¿Y por qué? La respuesta está relacionada a la cantidad de datos disponibles de manera gratuita, aunque limitada, en un formato estructurado. Diferente de las otras redes sociales, principalmente las controladas por el grupo Facebook, que son cerradas en relación a las publicaciones y datos de usuarios, el Twitter ofrece acceso gratuito a los datos, aunque de manera limitada.

En tecniqués: ser cerrada significa que no existe una forma gratuita de acceder a los datos de usuarios (contenido de sus publicaciones y perfil) de manera estructurada y que no viole los termos de uso de la plataforma. Ya el Twitter ofrece una API[2] en la cual es posible obtener informaciones sobre uno o varios perfiles en lote (s), además de los datos sobre sus actividades en la red: publicaciones, me gusta, comparticiones y metadatos, que pueden incluir geolocalización, idioma utilizado, foto del perfil, fecha y hora de la publicación y otras informaciones.[3]

[2] API - Application Programming Interface (Interfaz de Programación de Aplicaciones): una interfaz proyectada para el cambio de informaciones entre sistemas.

[3] Hay una versión gratuita y versiones pagas de la API de Twitter. La diferencia está en la cantidad de resultados que se pueden recuperar y sus metadatos.

IDENTIFICAR BOTS NO ES UNA RECETA DE PASTEL (AUN)

El uso de automatización ya es una realidad hace años e identificarla no es una tarea trivial. Un excelente ejemplo puede ser observado en el estudio realizado sobre el uso de automatización en WhatsApp durante las elecciones brasileñas de 2018. En la medida en que los estudios y técnicas para la detección evolucionan, también lo hacen las herramientas responsables de la automatización, en la misma velocidad o hasta mayor. Si pudiéramos elegir a alguien para echarle la culpa, ese alguien seria la demanda, pues ella existe y no es pequeña. Hay tanto el interés financiero inmediato, por parte de quien desarrolla la herramienta, cuanto el interés por influenciar masivamente en el debate público, por parte de quien consume y paga por ello. Como lo demuestra un reportaje de la revista Wired aun en 2017, y también algo similar relatado por la CNBC este año. La conclusión es que la automatización puede parecer algo lejano, pero no lo es. Si te has caído en paracaídas en el tema, siento decirte: hay bot para todo, desde ejecutar funciones como dar me gusta en una foto, hasta aumentar el número de seguidores a los bots que operan transacciones de compra y venta en bolsa de valores. Una vez que robot no duerme.

Todo eso para decir que: hay bastante cosa en juego, lo que torna la tarea de “cazar” e identificar ese comportamiento un interés de todos, de las plataformas donde las automatizaciones ocurren, de diferentes organizaciones de la sociedad civil e incluso de las instituciones democráticas, que se sienten amenazadas por el uso ilegal de bots durante períodos electorales, por ejemplo. De esa manera, la identificación de bots se convierte en una eterna pelea de perro y gato, a la manera Tom y Jerry, o una larga guerra compuesta por pequeñas batallas, visto que el hecho de que funcione hoy no significa que mañana funcionará con la misma seguridad y precisión. Las acciones de ambos lados están siempre en beta.

PROCESO DE ANÁLISIS: UNA ABSTRACCIÓN POSIBLE

Identificar un bot no es simple. No es como si pudiéramos tirar al alto una moneda y decir: “¡ES BOT!”. Hay muchos conceptos que deben ser considerados. Como estábamos hablando sobre el hecho de que no existe una receta de pastel lista para la detección de un bot, ¿intentamos construir algo que nos ayude en este camino?

NECESITAMOS DE:

a. La receta: un modelo de detección;

b. Ingredientes: los criterios;

c. Ejecutar la receta: girar el análisis combinando los criterios;

LO QUE TENDREMOS:

a. El pastel listo: comportamiento de bot detectado;

PASOS:

1. Tras separar los ingredientes (criterios) nuestro objetivo es combinarlos dentro de una secuencia de pasos. Atención para no añadir más fariña de lo necesario en relación a los demás ingredientes, sino creará desequilibrio (un falso positivo). El secreto es mantener la alquimia (equilibrio) entre los ingredientes (criterios).

2. Bate los ingredientes (gira el análisis), a mano o en la batidora (a partir de un método) y lleva al horno. Si todo ocurrir bien, tendrás un pastel lindo y sabroso (resultado concluido con el porcentual de comportamiento de bot de un perfil).

Nunca pensé que mis dotes culinarios y mi pasión por la tecnología podrían ser útiles en un artículo sobre bots.

¡¿ES UN BOT O NO LO ES?!

Sobre la detección de bots y comportamiento automatizado, fueron identificados diversos criterios que forman el conjunto de elementos que serán analizados en el proceso de detección. Los criterios son parte fundamental de la formula que contestará a la pregunta: ¿cuán bot ese perfil es considerado? Vamos a comprender algunos de esos criterios:

1. CARACTERÍSTICAS DEL PERFIL:

a. Actividad: el perfil es analizado por las características de su actividad, de la misma manera que los tipos de interacciones de la cuenta. Características sospechosas son: un histórico de actividad repetitiva, con publicaciones realizadas en intervalos cortos de tiempo o e horarios específicos del día. Investigadores de Oxford Internet Institute asumen que una cantidad superior a 5o tuits/día puede configurar un comportamiento automatizado.

b. Frecuencia: frecuencia, intervalo y tipo de publicaciones. Intervalos muy cortos (segundos o milisegundos), volumen muy alto de publicaciones y actividades muy repetitivas (normalmente, una cuenta que hace muchos retuits) indican alta probabilidad de automatización.

c. Nombre de usuario (su @): cuando el nombre de usuario, handle o arroba (@) posee una combinación entre dígitos y números, existe mayor posibilidad de que el usuario haya sido generado de manera automatizada.

d. Anonimidad: Presencia o ausencia de una foto de perfil y tipo de imagen utilizada. Perfiles que utilizan avatares ganan puntuación más elevadas en el análisis de probabilidad de automatización.

2. AMPLIFICACIÓN DE CONTENIDOS:

Contenidos que presentan alto número de compartición, aunque los perfiles tengan pocos seguidores, indican alta probabilidad de automatización.

3. ÉXITO:

Cuentas que poseen publicaciones con gran número de me gusta y retuits, a pesar de que la cantidad de seguidores sea muy baja, indican alta probabilidad de automatización.

4. CONTENIDO SUBIDO:

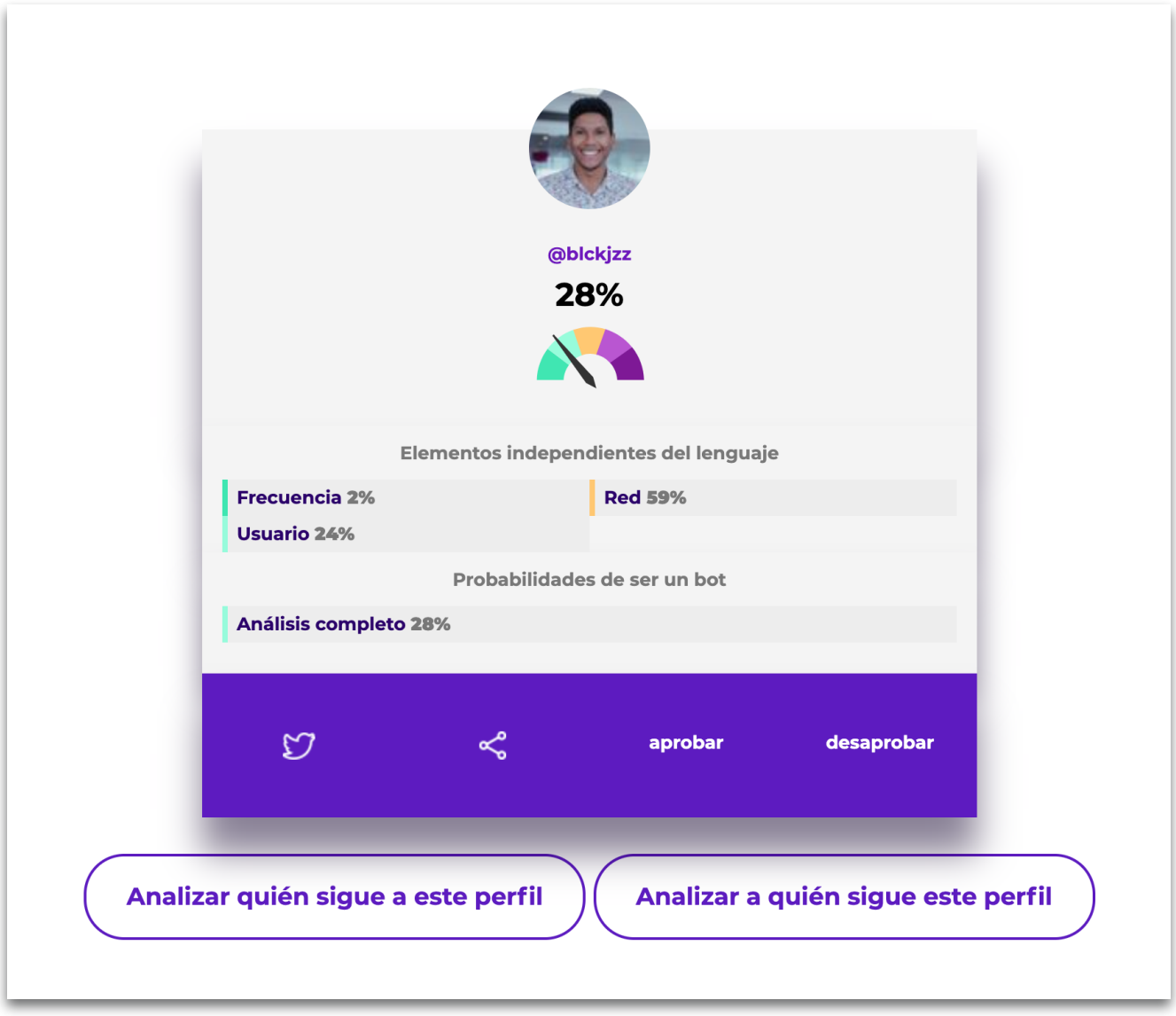
a. El análisis de sentimientos también suele entrar en la fórmula, generalmente realizando el análisis a partir de un conjunto de tuits subidos.

b. En un análisis lingüístico realizado a partir de algoritmos de Machine Learning para identificar patrones de lenguaje.

5. RED

Se realiza un análisis del flujo de las informaciones para entender como perfiles están siendo conectados y como diseminan contenido entre sí, con enfoque en las correlaciones.

Esa lista puede ser bastante extensa y tiene como objetivo dar un veredicto: cuán bot una cuenta o perfil es considerada. Esa es, por ejemplo, la tarea del Atrapabot, proyecto desarrollado por el ITS Rio e IT&E. Observen que en esta herramienta soy considerado 28% robot y el Atrapabot en ningún momento me clasifica como “bot” o “no bot” y punto final. Eso puede parecer raro, pero demuestra justamente que identificar un comportamiento de bot de manera automática (o sea, a partir de otro robot, como es el caso del Atrapabot) no puede representar un veredicto final. En última instancia, es la evaluación humana que tiene la capacidad de validar o reprobar el análisis.



Análisis de mi propio perfil del Twitter (@blckjzz) por la herramienta Atrapabot (https://es.pegabot.com.br)

Una vez que esos bots están cada vez más sofisticados, existe interés por parte de las propias plataformas en removerlos, pues causan perjuicos financieros milionarios, entre bots y cuentas falsas. Aun así, como ya ha sido mencionado, sus métodos de detección no son una “bala de plata” o “receta” lista que puede detectar y eliminar/reducir el comportamiento automatizado. Eso revela el tamaño de la dificultad de separar humanos y robts, sin que los propios usuarios de las plataformas sufran injusticia, ya que efectivamente poseen perfiles reales con gran volumen de publicaciones, baja frecuencia, muchos retuits y elevado alcance, por ejemplo. Todavía tenemos un largo trabajo adelante, ya que, hablando en el buen“carioqués”, robts hacen de todo para que puedan “pasarse desapercibido”.

REFERÊNCIAS

[1] BRADSHAW, S. et al. Sourcing and Automation of Political News and Information over Social Media in the United States, 2016-2018. Political Communication, v. 37, n. 2, p. 173–193, 3 mar. 2020.

[2] DAVIS, C. A. et al. BotOrNot. Proceedings of the 25th International Conference Companion on World Wide Web - WWW '16 Companion. [S.l: s.n.]. Disponível em: <http://dx.doi.org/10.1145/2872518.2889302>. , 2016

[3] @DFRLAB. #BotSpot: Twelve Ways to Spot a Bot. Disponível em: <https://medium.com/dfrlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c>. Acesso em: 2 abr. 2020.

[3] QI, S.; ALKULAIB, L.; BRONIATOWSKI, D. A. Detecting and Characterizing Bot-Like Behavior on Twitter. In: INTERNATIONAL CONFERENCE ON SOCIAL COMPUTING, BEHAVIORAL-CULTURAL MODELING AND PREDICTION AND BEHAVIOR REPRESENTATION IN MODELING AND SIMULATION, 10 jul. 2018, [S.l.]: Springer, Cham, 10 jul. 2018. p. 228–232. . Acesso em: 2 abr. 2020.

[4] VAROL, O., FERRARA, E., DAVIS, C. A., MENCZER, F., FLAMMINI, A. Online Human-Bot Interactions: Detection, Estimation, and Characterization. Eleventh international AAAI conference on web and social media, 27 mar. 2017. Disponível em: <https://arxiv.org/pdf/1703.03107.pdf>. Acesso em: 2 abr. 2020.

[5] WANG, Y.; WANG, L. Bot-like Behavior Detection in Online Banking. Proceedings of the 2019 4th International Conference on Big Data and Computing - ICBDC 2019. [S.l: s.n.]. Disponível em: <http://dx.doi.org/10.1145/3335484.3335518>. , 2019