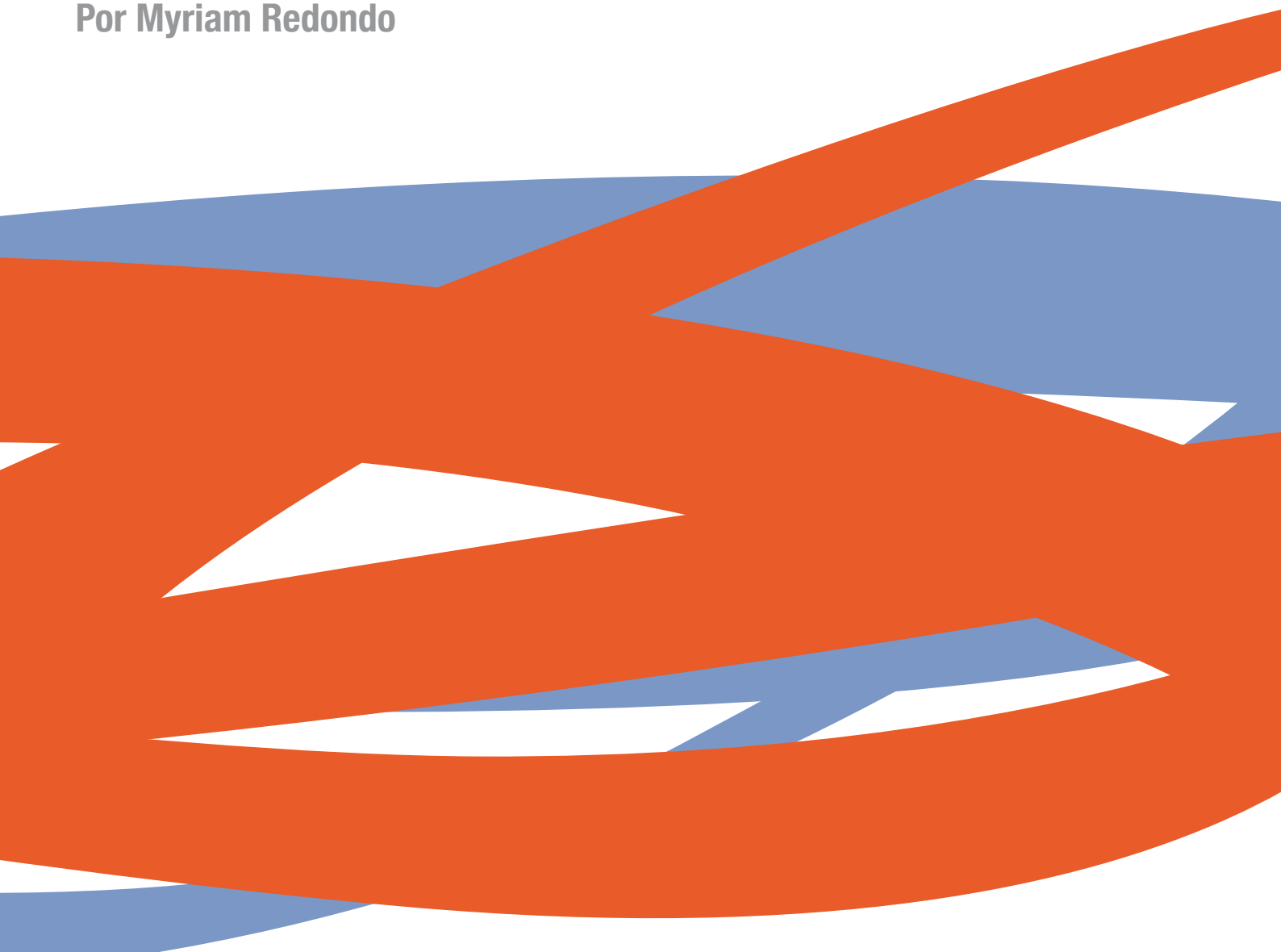
acop papers nº5

Política automatizada:

Bots, trols y propaganda digital encubierta en la **comunicación internacional**

Por Myriam Redondo



Myriam Redondo

Periodista *freelance* especializada en nuevas tecnologías para la comunicación internacional. En 2006 obtuvo el premio extraordinario de doctorado en Relaciones Internacionales con una tesis que analizaba el uso de Internet como fuente de información entre los corresponsales y las instituciones comunitarias. Ha sido colaboradora de medios que van de Ciberpaís a la revista Economía Exterior, editora web, profesora universitaria y asesora de comunicación ministerial en las áreas de Ciencia, Innovación y Educación. Actualmente centra sus investigaciones en la propaganda digital y la verificación de contenidos amateur (eyewitness media) para evitar la desinformación. Es miembro del comité editorial de la revista de ACOP.

Resumen:

El recurso a la propaganda automatizada (basada en robots o *bots* digitales) se ha reportado ya en cerca de 40 países y en 100 operaciones de diseño político. Las prácticas más suaves se dirigen a aumentar el número de seguidores de un líder; las más dañinas incorporan cuentas falsas gestionadas por humanos cuyo objetivo es manipular, anular debates incipientes, alterar comicios o paralizar mediante la confusión. El debate sobre el uso o la proscripción de los bots y la desinformación que los acompaña es un desafío para la comunicación política y otros campos académicos como el periodismo, la informática o la psicología.

Contacto

Mail: globograma@gmail.com

Twitter: @globograma

Palabras claves:

Política automatizada, propaganda, desinformación, *bots*, Internet, trols, campañas electorales, comunicación internacional, ética, comunicación política

ACOP Papers ISSN 2445-396X

ANTECEDENTES

En abril de 2016, un pirata informático con el aire inquietante de Walter White, el protagonista de la serie Breaking bad, denunciaba desde la portada de Bloomberg BusinessWeek haber pasado ocho años alterando campañas electorales en América Latina. Sus tácticas incluían el envío masivo de mensajes a las redes sociales. En al menos 40 países se han observado ya prácticas de este tipo, basadas en robots, pero la capacidad de manipulación de la "política automatizada" se basa sobre todo en la sofisticación de la propaganda humana con que se suele completar.

Los *bots* (acortamiento del término robot) son programas o conjuntos de reglas informáticas que recorren la Red ejecutando acciones automáticas. Su diseño conlleva ingenio e innovación. Sustentan muchos servicios útiles, desde el rastreo de webs por parte de buscadores hasta el envío personalizado de noticias. Artistas, activistas, plataformas ciudadanas, partidos, empresas, gobiernos, ejércitos y cualquier otra institución pública o privada pueden lanzar iniciativas beneficiosas o legítimas mediante *bots*. No son ilegales.

Con carácter general, la propaganda automatizada podría definirse como el conjunto de prácticas ejecutadas por programas informáticos para persuadir de las bondades de ideas, personas o iniciativas. En la política automatizada, esos programas han sido diseñados con fines políticos.

Como explica Antoni Gutiérrez Rubí en el monográfico nº 2 de ACOP (Política: del big data al data thinking) la tecnología y la inteligencia de datos ofrecen oportunidades indudables al campo de la comunicación política y la gestión de Gobierno, permitiendo convertir la información en conocimiento útil para solventar retos sociales. Ese debe ser el acercamiento, pero los algoritmos o fórmulas informáticas tras algunos *bots* se alejan de esa honestidad tecnológica por un rasgo esencial: el ciudadano desconoce su carácter planificado y su propósito.

Tradicionalmente se ha distinguido entre propaganda blanca, gris y negra. Si en la primera la fuente se identifica, sin temer evidenciar su propósito de promoción mediante argumentos escorados, la política automatizada se acerca a las propagandas gris y negra, en las que los organizadores ocultan su origen o falsean el mismo, quedando protegidos a la hora de difamar, manipular o mentir. También son plausibles las iniciativas de "bandera falsa" en las que se atribuye al contrincante el origen de la operación.

BOTS Y CUENTAS FALSAS

Algunos tienen la única función de retuitear contenidos ajenos. Otros pueden adquirir uno o varios de los siguientes rasgos:

- Apertura de múltiples cuentas en distintas redes sociales.
- Publicación automática en ellas de mensajes basura (spam) o de mensajes idénticos (twitterbombing).
- Funcionamiento zombi. Letargo durante largos periodos hasta el lanzamiento unánime de una corriente para lograr temas destacados (trending topics) o vuelcos en los resultados de búsqueda de un término.
- Mimetismo o imitación de comportamientos humanos.
- Usurpación de personalidades ajenas -incluso internautas fallecidos- preferiblemente atractivas; un recurso frecuente son las fotografías de perfil de celebridades.
- Corrupción de los hashtags o etiquetas con las que se identifican los hilos temáticos en las redes sociales (hashtag spamming) mediante el lanzamiento masivo de mensajes que las usan sin sentido. Así la etiqueta va perdiendo relevancia porque sus impulsores dejan de usarla, los tuiteros que llegan de nuevas no las entienden o Twitter las anula. Paralelamente, se lanzan otras etiquetas que difunden el pensamiento propio (guerras de spam).
- Persistencia y sistematicidad.

Algunos *bots* son difíciles de detectar. Abordan asuntos desde un punto de vista muy positivo o muy negativo, no dan respuesta cuando se les formula una pregunta directa… En Twitter no suelen indicar localidad o zona horaria ni tienen favoritos. Si presentan listas, están llenas de usuarios ajenos a su supuesta especialización. Hay herramientas que identifican los *bots* ocultos entre los seguidores de una cuenta (Theblockbot.com, Twitteraudit.com) y el test más avanzado para comprobar si un usuario de Twitter tiene rasgos de bot puede ser BotOrNot (http://truthy.indiana.edu/botornot/). Pero aún no existe la herramienta perfecta.

El verdadero impacto de los *bots* llega cuando se combinan automatismos con acciones humanas. Por ejemplo, pueden alterarse levemente los mensajes para evitar los filtros antispam. Y hay campañas en las que se contrata a blogueros o tuiteros habilidosos que operan con normalidad: escriben sobre libros, películas o memes populares hasta que reciben la indicación de tratar determinado asunto. Otra opción es contar con ellos para ejercer de trols o mantener perfiles ficticios (cuentas falsas o sockpuppets).

Los trols existen desde el inicio de Internet y su misión primigenia era incordiar y desbaratar conversaciones ajenas. Los perfiles ficticios, que simulan una identidad, suelen ser exageradamente amables con figuras relevantes. Al ganarse su confianza y lograr interactuar con ellos obtienen la visibilidad y reputación que estos influencers les proporcionan. En ocasiones una sola persona puede manejar 20 o 30 cuentas falsas e incluso hacer que hablen entre ellas para dar veracidad a la discusión.

Los objetivos de las campañas automatizadas/humanas -que se pueden dirigir a votantes propios, votantes del partido contrario o a la ciudadanía en general- son los siguientes:

- Desinformar y expandir rumores y falsas impresiones, confundiendo la conciencia colectiva y paralizando mediante la duda, especialmente en estados de incertidumbre política o social.
- Debilitar ideas que empiezan a adquirir cuerpo social y malograr debates incipientes, impidiendo que se configuren conversaciones organizadas y lógicas.
- Desmovilizar, frustrar protestas ya iniciadas.
- Desestabilizar y provocar cambios de tendencia en los procesos electorales.
- Exagerar la fortaleza de un partido/régimen o aumentar artificialmente la popularidad de un candidato/líder, haciendo invisible a su contrincante o destrozando su reputación.
- Ahogar críticas a autoridades, sistemas políticos o estructuras del Estado.
- Silenciar ataques a los derechos humanos o el recurso a la violencia.
- Espiar a disidentes y detectar posibles infracciones de la ley.
- Impedir la libertad de expresión. Censurar.

En un contexto de presencia creciente de los contenidos digitales generados por usuarios (CGU), periodistas y ciudadanos lo tienen cada vez más difícil para verificar qué vídeos o qué corrientes de opinión triunfantes son genuinas y cuáles inducidas. Las campañas pseudoespontáneas proliferan. En ellas el mensaje está muy dirigido pero parece haberse originado en individuos de la comunidad sin intereses creados ni relación concreta con ninguna organización. Los anglosajones denominan a esta práctica Astroturfing a partir de la marca de un césped artificial así llamado y como juego de palabras con las acciones *grassroot*, de base o de raíz.

Los avances en algoritmos e inteligencia artificial hacen que se perfeccionen las campañas. Las cifras hablan de operaciones a gran escala y elevan los *bots* a la categoría de fenómeno transnacional, aunque hay que puntualizar que muchos de ellos están inactivos. Facebook pasó de los 83 millones de cuentas falsas de 2012 a los 170 de 2014. Ese mismo año, Twitter reconoció en una estimación que se consideró muy conservadora unos 13 millones de usuarios no reales. En 2013, los *bots* generaban un 61% del tráfico web, según la consultora de seguridad Incapsula. El porcentaje se ha reducido en los

años siguientes, con los humanos recuperando la mayoría activa, pero en las redes la presencia de las máquinas es evidente.

Algunas de las investigaciones más avanzadas sobre el impacto de los bots en la vida pública parten del Proyecto sobre Propaganda Automatizada (politicalbots.org), apoyado por la Universidad de Washington y el Instituto de Internet de Oxford y encabezado por el profesor Phil Howard. OSoMe (truthy.indiana.edu), observatorio de la Universidad de Indiana coordinado por los investigadores Filippo Menczer y Alessandro Flammini, se centra en las campañas organizadas que se presentan como espontáneas. La Iniciativa de Autonomía e Inteligencia (autonomy.datasociety.net), con respaldo de la Fundación Soros y la Fundación Bill y Melinda Gates, también investiga para garantizar el interés público en los dominios que vinculan robots, algoritmos y automatización.

En España, la referencia es "*Bots* de Twitter" (botsdetwitter.wordpress.com y @botspoliticosno). Su objetivo es desenmascarar a los impulsores de estas tácticas para que tengan que cerrar sus cuentas o Twitter las suspenda. En 2015 detectaron 20 redes de mensajes basura políticos que totalizaban 1.060 perfiles falsos. La actividad más intensa que registraron fue contra el movimiento independentista en Cataluña. @Botspoliticosno ha localizado mayor número de *bots* en campañas a favor del Partido Popular, pero advierte que son empleados por todas las ideologías políticas. La última red que identificaron, activa en febrero de 2016, emitió primero tuits favorables al PSOE y luego otros contra un posible pacto PSOE-Podemos.

PANORAMA INTERNACIONAL

Politicalbots.org habla de *bots* encontrados en unos 40 países y de cerca de 100 casos donde su intención era claramente política (Sam Woolley, "Automating power: social bot interference in global politics", 2016). Estos son algunos países donde prensa e internautas han reportado el

recurso a la propaganda automatizada:

- **Corea del Sur.** En el año previo a las elecciones de 2012, los servicios de inteligencia del país (NIS) enviaron más de 22 millones de tuits entre los que muchos apoyaban a la candidata Park Geun-hye, que se hizo con la presidencia. Se negaron oficialmente las numerosas acusaciones y se dijo que el único propósito de los mensajes era hacer propaganda contra el enemigo tradicional, Corea del Norte, pero la fiscalía inició un proceso y terminó encarcelando al responsable del NIS.

> *"Los avances en algoritmos e inteligencia artificial hacen que se perfeccionen las campañas*

- **Estados Unidos.** Ya en 2010 los investigadores Panagiotis T. Metaxas y Eni Mustafaraj observaron la manipulación de los resultados en buscadores ante unas elecciones celebradas en Massachusetts. Ese mismo año, cerca de 20.000 mensajes salieron de sólo dos cuentas de Twitter con enlaces a la web del político John Boehner. En 2011 se atribuyeron *bots* al candidato Newt Gingrich y también a la web simpatizante Freedomist.com. En 2012 se sospechó de los 116.000 seguidores que Mitt Romney ganó en un día. Más recientemente, en los cáucuses de Nevada aparecieron numerosas cuentas de seguidores latinos tuiteando idénticos mensajes favorables a Donald Trump. Y se han hallado también Obamabots, aunque en la estrategia del presidente de EEUU parece primar el sistemático tuiteo "humano" de los activistas reales sobre las cuentas automáticas.

- **Turquía**. Se han utilizado *bots* favorables al Partido de la Justicia y Desarrollo, al que pertenece el presidente Recep Tayyip Erdoğan, pero también al opositor Partido Republicano del Pueblo. El equipo de Erdogan, quien ha llegado a decir que las redes sociales son "la peor amenaza para la sociedad", anunció la contratación de 6.000 activistas en las elecciones locales de marzo de 2014 para promover acciones en Red. Los investigadores Peter Nut y Dieter Leder descubrieron que también se abrieron 18.000 cuentas falsas pro-Erdogan en solo un mes. La propaganda automatizada aumentó tras las "protestas de Gezi" contra la brutalidad policial.

- **Venezuela**. Nicolás Maduro es la tercera personalidad pública más retuiteada del mundo, tras el Papa y el Rey de Arabia Saudí, según la consultora Burston Marsteller. El presidente de Venezuela, Nicolás Maduro, se ha quejado del cierre de cuentas de seguidores (Twitter ha clausurado más

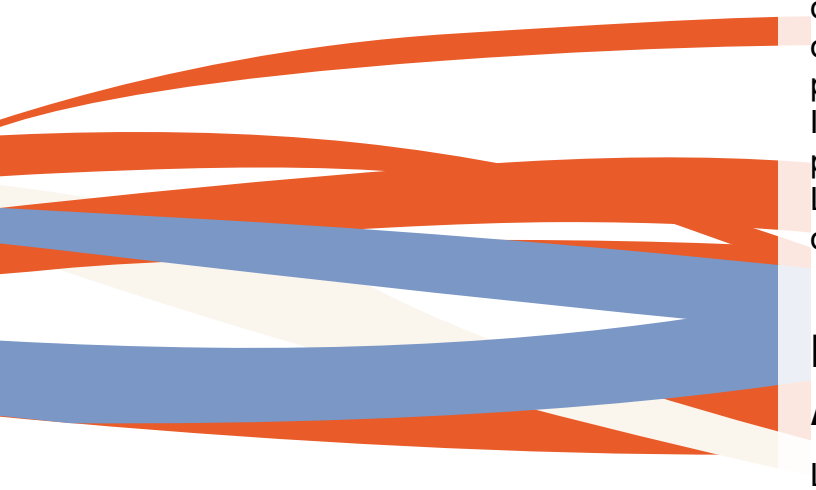
de 6.000) pero explora los límites de lo que sería activismo legítimo a la hora de difundir consignas antiimperialistas con etiquetas como #ObamaYankeeGoHome. Los seguidores de Maduro tienen a su disposición una aplicación móvil para retuitear automáticamente desde sus cuentas cada mensaje del líder. El investigador Kyumin Lee habla de "alianza de *bots*" en el país.

México y Rusia son dos de los países donde los *bots* han tenido mayor resonancia. En México se ha acusado a los tres grandes partidos de tácticas automatizadas encubiertas, pero las acusaciones más sistemáticas se producen contra los "Peñabots" (que favorecen al presidente, Enrique Peña Nieto). Han llegado a promover tres tendencias falsas al día, según el programador web anti-priísta Iván Santiesteban. Los expertos en redes Erin Gallagher y Alberto Escorcia hablaban en agosto de 2015 de 75.000 cuentas automatizadas en el país, que ha vivido sangrientas guerras de etiquetas. Si ciudadanos conmocionados por la desaparición de 43 estudiantes en Ayotzinapa canalizaban su ira con la expresión #YaMeCansé, ésta era rápidamente inutilizada con spam sin sentido. Si se extendía la etiqueta #RompeElMiedo para ubicar a la policía y evitar encuentros con ella en manifestaciones, sucedía lo mismo. Otros ejemplos de esta tendencia fueron #SobrinaEPN o #YoSoy132, ambas originalmente críticas con el presidente.

> *"México y Rusia son dos de los países donde los bots han tenido mayor resonancia.*

En Rusia el recurso a los *bots* comenzó a visibilizarse en 2011 para acallar el malestar por las acusaciones de fraude en las elecciones legislativas. Lawrence Alexander, colaborador del sitio ciudadano Global Voices, detectó en 2015 cerca de 20.500 cuentas automatizadas a favor del Kremlin. Tras el asesinato del líder opositor Boris Nemtsov se activaron para silenciar la protesta que se inició en las redes. Rusia también está profundizando en la propaganda digital encubierta realizada por humanos. La crónica de The New York Times "The Agency" (2015) no tiene desperdicio. Refleja las vicisitudes del reportero Adrian Chen para introducirse en los bajos fondos de lo que se han llamado "fábricas de trols" o "granjas de trols" rusas, empresas que contratan confidencialmente a jóvenes para ejercer de trols bajo consignas políticas que se les reparten cada día. Se acusa a Moscú de elevar a niveles industriales el arte de la desinformación en RuNet, la Internet rusa. Está en juego "la utilidad misma de Internet como espacio democrático", dice Chen.

El hacker que habló para Bloomberg BusinessWeek, Andrés Sepúlveda, encarcelado por espionaje en Colombia, afirmó haber intervenido en este país, en México y en Venezuela, pero también en Nicaragua, Panamá, Honduras, El Salvador, Costa Rica y Guatemala. Se han reportado prácticas de automatización en Arabia Saudí, Argentina, Australia, Azerbaiyán, Baréin, Canadá, Irán, Italia, Marruecos… En China, cerca de 448 millones de comentarios son publicados cada año en las redes sociales



para promocionar al gobierno ("How the Chinese government fabricates social media posts for strategic distraction, not engaged argument"; G. King, J. Pan y E. Roberts, 2016). Los *bots* y trols están presentes en la guerra de Siria y la actividad del Estado Islámico, insertados en la tradicional maquinaria de guerra de la información y operaciones psicológicas que caracteriza a todos los conflictos.

Los ejemplos aportados reflejan que los *bots* también se emplean en países democráticos, aunque en ellos tiendan a protagonizar prácticas consideradas suaves como aumentar el número de seguidores de un líder o deslucir al adversario. Las dictaduras o países de democracia no consolidada han virado hacia prácticas más virulentas relacionadas con el robo de datos, la vigilancia ciudadana y el espionaje a opositores internos o estados enemigos mediante programas malignos (malware).

"Mi trabajo era hacer acciones de guerra sucia y operaciones psicológicas, propaganda negra, rumores, en fin, toda la parte oscura de la política", decía Sepúlveda. Es pura tecnocensura alejada por completo de la comunicación política. En julio de 2015 hackers anónimos dieron a conocer documentación interna de la empresa italiana de software intrusivo Hacking Team, calificada por Reporteros sin Fronteras como "enemiga de Internet" por facilitar aplicaciones de vigilancia a países que no respetan los derechos humanos. Los estados con mayores contratos, según se desveló, eran México, Italia y Marruecos.

EL FUTURO DE LA POLÍTICA AUTOMATIZADA

La mayoría de los estudios sobre el uso de *bots* se basan en denuncias de internautas o de los periodistas (politicalbots.org detecta sus casos de análisis en las noticias de medios reputados). Excepcionalmente, hablan trols o hackers arrepentidos o hay entrevistas con fuentes anónimas de alto nivel. La falta de pruebas es una de las principales dificultades para acabar con la propaganda automatizada. Frecuentemente se captan en las redes pantallazos difícilmente irrefutables de las malas prácticas, pero es difícil vincularlas a instancias oficiales o aparatos políticos. Y el hecho de que una campaña beneficie a un partido no siempre significa que éste la pusiera en marcha.

> *"Que una campaña beneficie a un partido no siempre significa que éste la pusiera en marcha*

En ocasiones se concreta la intervención de algún responsable de comunidades (community manager) que actuó a favor de un político concreto, no del partido. Pero lo habitual es que aparezcan en el paisaje sucesivos intermediarios, subcontrataciones encadenadas o expertos externos, lo que permite al líder de la formación bajo sospecha asegurar que no sabía nada y deja en el aire la moralidad de unos trabajos de asesoría que a veces fueron contratados con dinero público. Las cuentas señaladas como *bots* cambian de foto de perfil, borran los tuits más comprometedores o paran durante un tiempo. Eso puede ser todo.

La confusión aumenta cuando la fuente

original del mensaje es un simpatizante que actúa como lobo solitario digital, al margen del partido. Algunos torbellinos de desinformación son verdaderamente complejos. Mari Luz Congosto y Antonio Delgado analizaron para El Español la expansión de la etiqueta #DesmontandoaCiudadanos. Un usuario proclive a Podemos publicó un vídeo de 16 minutos crítico con la formación de Albert Rivera. En 24 horas se convirtió en tendencia tras numerosos retuiteos, sobre todo desde las redes de Podemos. Ciudadanos denunció que se trataba de una campaña de *bots* realizada desde Venezuela en conexión con el partido de Pablo Iglesias. Éste lo negó. Congosto y Delgado detectaron sólo 20 *bots* frente a decenas de miles de cuentas humanas que utilizaron la etiqueta en cuestión. Algunos perfiles procedían efectivamente de Venezuela, pero se habían sumado a ese tema del día porque es práctica habitual hacerlo para publicitar los contenidos propios de manera oportunista.

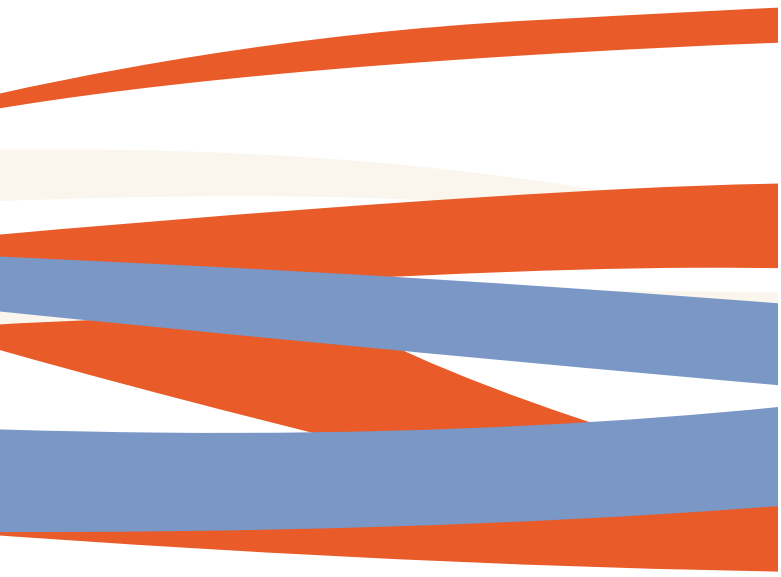
> **"Provocar cambios radicales de opinión a través de la automatización no es tan fácil**

¿Cómo afectan estas campañas políticas al comportamiento electoral? ¿Funciona la manipulación? ¿Cuál es su verdadero impacto? "Lo más escalofriante es cuando hablas con tus amigos y están repitiendo las mismas cosas que viste en tu argumentario, y te das cuenta de que todo eso está teniendo un efecto", explicaba una trol rusa arrepentida a The Guardian tras abandonar una oficina oculta en la que tuiteaba contra Barack Obama o el presidente de Ucrania, Petro Poroshenko.

La mayoría de los expertos tranquilizan sobre la cuestión. Provocar un vuelco electoral o cambios radicales de opinión a través de la automatización no es tan fácil. Por varios motivos: a) muchos votantes viven todavía al margen de la Red –la mitad de la población mundial aún no accede a ella- y por tanto son ajenos a estas influencias; b) los análisis de redes avanzan y permiten desmontar más rápidamente las corrientes automáticas (las etiquetas que se expanden espontáneamente suelen estar impulsadas por usuarios conectados entre sí, mientras las planificadas se distribuyen a partir de nodos separados); c) si cada vez hay *bots* más perfeccionados puede pensarse que también habrá mejores herramientas para detectarlos; d) la prensa muestra creciente avidez ante las tácticas de propaganda automatizada, buscando el escarnio de los impulsores; e)

a medida que aumente la conciencia crítica de los ciudadanos con respecto a temas tan sensibles como el uso de datos personales o la manipulación de algoritmos, el recurso a estas prácticas tendrá un enorme coste para la imagen de los políticos infractores; f) hacerse con un servicio de *bots* sale más barato que contratar un anuncio de televisión, pero como recuerda Tom Trewinard ("Sockpuppets and spambots: how states manipulate social networks", 2016) una campaña de desinformación bien elaborada, con intervención humana, requiere mucho tiempo y esfuerzo; g) algunos estudios sugieren que la crítica espontánea sigue venciendo al automatismo a la hora de valorar propuestas o productos en Internet; otros revelan que los rumores se extienden con rapidez en línea pero que también lo hace la colaboración para desenmascararlos.

Muchas de las operaciones que se han descrito en este texto tienen que llegar a millones de personas para lograr el impacto que buscan, y por tanto podrían quedar reservadas a la dimensión estatal o internacional. Pero fijar límites éticos a la propaganda automatizada debería ser un objetivo incluso en microentornos locales. Es una cuestión interdisciplinar que interesa a la informática, el derecho, la psicología, la sociología y por supuesto la comunicación política.



En la revista Salon, Tim Hwang y Samuel Woolley proponen una autoregulación que incentive el buen uso político de los *bots*. Estaría basada en un ecosistema abierto con instituciones que confiesan el origen, diseño y uso de *bots* y renuncian a prácticas de confusión entre *bots* y humanos. En ese ecosistema plataformas como Twitter y Facebook, acusadas de actuar sólo cuando algún caso alcanza sonoridad escandalosa, abandonarían su escudo de neutralidad habitual para colaborar más activamente en la detección y anulación de las cuentas automáticas. Yendo más lejos, @ Botspoliticosno pide "tolerancia cero hacia los *bots*".

El objetivo de los automatismos con intervención humana mencionados aquí no es articular "la toma de decisiones políticas así como la aplicación de estas en la comunidad", como ocurre con el intercambio de mensajes poder-ciudadanía y ciudadanía-poder en la comunicación política (Comunicación Política, una guía para su estudio y práctica, Mª José Canel, 2006). Y si los *bots* no son comunicación política, la política automatizada no es tampoco política. Si se entiende esta como ejercicio profesional centrado en la gestión del bien común, de lo que debería hablarse es de antipolítica.

Las operaciones descritas se alejan del activismo legítimo que hacen las juventudes de los partidos o de los movimientos que se coordinan vía Telegram para crear trending topics a horas concretas. Tampoco son inteligencia de datos dirigida a detectar necesidades sociales y a desarrollar iniciativas que las solventen. No hay beneficios para los ciudadanos. Los *bots* no están significando sólo automatización, sino maquinación.

*Agradecimientos a la investigadora Mariluz Congosto (@congosto) y a otros expertos por sus comentarios durante la realización de este monográfico.

acop

asociación comunicación política