Biblioteca del Congreso Nacional de Chile

Los Bots en las Redes Sociales y los Riesgos para la Democracia

Serie Informes Nº 31-22, 29/11/2022

por Marek Hoehn

Resumen

El presente Informe fue elaborado para entregar antecedentes sobre las definiciones y características de los bots en general y los social bots en particular. El informe entrega información sobre su funcionamiento, sus usos, su relevancia y sobre los efectos de su utilización para la formación de la opinión pública así como los procesos de toma de decisión democráticos.

A modo de anexo presentamos un resumen del escándalo Facebook – Cambridge Analytica.

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: mhoehn@bcn.cl, Anexo: 1868

Tabla de contenido

1. Definiciones y delimitaciones

El concepto "robot" describe una herramienta programable capaz de ejecutar una serie de acciones complejas de manera autónoma. El origen etimológico se encuentra en la palabra "*robota*" o "*rabota*" que en las lenguas eslavas refiere al trabajo y fue aplicado a los campesinos obligados al servicio obligatorio en el contexto del sistema feudal.

El anglicismo "*bot*" es la forma abreviada de "*robot*". La versión corta es utilizada, principalmente, para diferenciar los robots mecánicos de aquellos constituidos meramente por código de programación (*scripts*). A estos últimos se suele referir como "*software agents*", "*software robots*" o simplemente "*bots"*.

El presente informe solo analizará los "*software robots*" o "*bots*". De acuerdo al pedido de asesoría no haremos referencia a los robots mecánicos. También, a partir de este momento, trataremos el anglicismo como palabra castellanizada, dejando de usar comillas y cursivas.

Todos los bots son programas computacionales. Como tal son una secuencia de instrucciones en un lenguaje de programación (*script/ code*) para ser ejecutado en un computador. Pero no todos los programas computacionales son bots. Los atributos básicos de un bot son que éstos:

- no son ejecutados manualmente para una tarea, sino que se activan por sí mismos
- pueden permanecer en estado de espera en un *host*, percibiendo el contexto,
- pueden llegar al estado de ejecución en un *host* al darse las condiciones de inicio,
- no requieren la interacción del usuario,
- pueden ejecutar otras tareas, incluida la comunicación.

En otras palabras, los bots son una entidad de software compleja que es capaz de actuar con cierto grado de autonomía para realizar tareas en nombre de su anfitrión. En la literatura parece haber consenso sobre cuatro características centrales de los bots:

1) Su persistencia. Esto implica que el código no es ejecutado *on demand*, sino que se encuentra en ejecución continuamente y decide por sí mismo cuándo debe realizar alguna actividad.
2) Su autonomía. Lo que hace referencia a que los bots tienen capacidades de selección de tareas, priorización, comportamiento dirigido a objetivos, toma de decisiones sin la necesidad de la intervención humana.
3) Su capacidad social. Es decir, los bots son capaces de involucrar a otros componentes mediante algún tipo de comunicación y coordinación, pueden colaborar en una tarea.
4) Su reactividad. Lo anterior implica que los bots perciben el contexto en el que operan y reaccionan a él adecuadamente.

Franklin y Graesser (1997) definen cuatro nociones clave que distinguen a los bots (recuerde: "*software agents*") de los programas comunes ("*common software*"):

a) reacción al entorno,
b) autonomía,
c) orientación a objetivos y
d) persistencia.[1]

2. Tipos de bots

De acuerdo a sus características, funcionamiento, objetivos, efectos y relevancia, los bots pueden ser agrupados en distintas categorías analíticas. Estas no son excluyentes y resaltan seleccionadas características, según el autor. La literatura propone las siguientes categorías, pero la lista está lejos de ser exhaustiva:

2.1 Internet bot

Un bot de Internet o "*web robot*" es una aplicación de software que ejecuta tareas automatizadas a través de Internet, normalmente con la intención de imitar la actividad humana en Internet, como la mensajería, a gran escala. Un bot de Internet desempeña el papel de cliente en un modelo cliente-servidor, mientras que el papel de servidor lo suelen jugar los servidores web.

Los bots de Internet son capaces de realizar tareas, que son simples y repetitivas, mucho más rápido de lo que podría hacer una persona humana. El uso más extendido de los bots es el rastreo de la web (*web crawling*), en el que un *script* automatizado obtiene, analiza y archiva información de los servidores web. Más de la mitad del tráfico web es generado por bots y casi la tercera parte de estos bots son considerados maliciosos.[2]

Los esfuerzos de los servidores web para restringir los bots varían. Algunos servidores tienen un archivo `robots.txt` que contiene las reglas que rigen el comportamiento de los bots en ese servidor. Cualquier bot que no siga las reglas podría, en teoría, ser negado el acceso o eliminado del sitio web afectado. Pero, si el archivo de texto publicado no tiene ningún programa/software/aplicación asociado, la adhesión a las reglas es totalmente voluntaria. No habría forma de hacer cumplir las normas ni de garantizar que el creador o ejecutor de un bot lea o acepte el archivo `robots.txt`.

Algunos bots son muy funcionales, por ejemplo, los "*web crawlers*" de las maquinas de búsqueda de Internet, ya que sistemáticamente revisan y registran la *World Wide Web* para efectuar su indexación con la que la búsqueda se efectúa de manera sumamente rápida.

Otros bots son más bien disfuncionales (o francamente maliciosos) porque son utilizados para lanzar ataques maliciosos contra, por ejemplo, las campañas

1 Franklin, S.; Graesser, A. (1996). "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents". Intelligent Agents III Agent Theories, Architectures, and Languages. Lecture Notes in Computer Science. Vol. 1193. University of Memphis, Institute for Intelligent Systems. pp. 21–35. doi:10.1007/BFb0013570. ISBN 978-3-540-62507-0.

2 Bot Traffic Report 2016: https://www.incapsula.com/blog/bot-traffic-report-2016.html

políticas.

Existen bots maliciosos (y redes de bots) de los siguientes tipos:

- *Spambots* que recogen direcciones de correo electrónico de las páginas de contacto o del libro de visitas
- Programas de descarga que ocupan todo el ancho de banda descargando sitios web enteros, haciendo imposible el uso de Internet
- *Scrapers* de sitios web que toman el contenido de los sitios web y lo reutilizan sin permiso en páginas de entrada generadas automáticamente
- Robots de registro que inscriben una dirección de correo electrónico específica en numerosos servicios para que los mensajes de confirmación inunden la bandeja de entrada del correo electrónico y distraigan de los mensajes importantes que indican una violación de la seguridad.
- Virus y gusanos
- Ataques DDoS. En informática, un ataque de denegación de servicio (ataque DoS) es un ciberataque en el que el autor intenta que el recurso de red (sitio web) no esté disponible para sus usuarios previstos, interrumpiendo temporal o indefinidamente los servicios de un *host* conectado a una red. La denegación de servicio se suele llevar a cabo inundando el servidor o el recurso objetivo con peticiones superfluas en un intento de sobrecargar los sistemas e impedir que se cumplan algunas o todas las peticiones legítimas. En un ataque de denegación de servicio distribuido (ataque DDoS), el tráfico entrante que inunda a la víctima se origina en muchas fuentes diferentes. Se requieren estrategias más sofisticadas para mitigar este tipo de ataque, ya que el simple intento de bloquear una sola fuente es insuficiente porque hay múltiples fuentes.
- Redes de bots, computadores zombies, etc.
- *Spambots* que intentan redirigir a la gente a un sitio web malicioso, que a veces se encuentran en las secciones de comentarios o foros de varios sitios web
- *Viewbots* que crean vistas falsas y bots que aumentan las visitas a los vídeos de YouTube, aumentando ganancias publicitarias
- Bots que compran los asientos más demandados para los conciertos, especialmente por parte de los corredores de entradas que los revenden. Estos bots recorren el proceso de compra de los sitios de venta de entradas para eventos de entretenimiento y obtienen mejores asientos retirando todos los que pueden.
- Los bots que se utilizan en los juegos de rol multijugador masivos en línea para cultivar recursos que, de otro modo, requerirían mucho tiempo o esfuerzo para obtenerlos, lo que puede suponer un problema para las economías en línea del juego.
- Bots que aumentan los recuentos de tráfico en los informes analíticos para extraer dinero de los anunciantes. Un estudio de Comscore descubrió que más de la mitad de los anuncios mostrados en miles de campañas entre mayo de 2012 y febrero de 2013 no se sirvieron a usuarios humanos.
- Bots utilizados en foros de Internet para publicar automáticamente

mensajes incendiarios o sin sentido para perturbar el foro y enfadar a los usuarios.

2.2 Spambot

Un spambot es un programa informático diseñado para recopilar direcciones de correo electrónico de páginas de contacto o de libros de visitas y ayudar al envío de spam. Los spambots suelen crear cuentas y enviar mensajes de spam con ellas.

El spamming es el uso de los sistemas de eMail o mensajería instantánea para enviar múltiples mensajes no solicitados (spam) a un gran número de destinatarios con fines de publicidad comercial, con fines de proselitismo no comercial, con cualquier fin prohibido (especialmente el fin fraudulento de la suplantación de identidad o *phishing*), o simplemente enviando repetidamente el mismo mensaje al mismo usuario.

Los anfitriones de la web y los operadores de sitios web han respondido prohibiendo el envío de spam, lo que ha dado lugar a una lucha continua entre ellos y los spammers en la que éstos encuentran nuevas formas de evadir las prohibiciones y los programas antispam, y los anfitriones contrarrestan estos métodos.

2.3 Comercial bot

Ha habido una gran controversia sobre el uso de bots en una función de comercio automatizado. El sitio web de subastas eBay emprendió acciones legales en un intento de impedir que una empresa de terceros utilizara bots para buscar gangas en su sitio. Este planteamiento resultó contraproducente para eBay y atrajo la atención de más bots.

La plataforma de apuestas, Betfair, con sede en el Reino Unido vio tal cantidad de tráfico procedente de bots que lanzó una API de servicio web dirigida a los programadores de bots, a través de la cual puede gestionar activamente las interacciones de los bots.

Se sabe que las granjas de bots se utilizan en las tiendas de aplicaciones en línea, como la App Store de Apple y Google Play Store, para manipular las posiciones o aumentar las valoraciones/revisiones positivas.

2.4 Trading bot

Un trading bot es un sistema de operaciones automatizadas para el *trading* en la bolsa de comercio. Como tal es un programa informático para crear órdenes de compra y venta y las envía automáticamente a un centro de mercado o a una bolsa. El programa informático generará automáticamente órdenes basadas en un conjunto de reglas predefinidas utilizando una estrategia de negociación que se basa en el análisis técnico, en cálculos estadísticos y matemáticos avanzados o en la información procedente de otras fuentes electrónicas.

Los sistemas de operaciones automatizadas se utilizan a menudo con la negociación electrónica en centros de mercado automatizados, incluidas las redes de comunicación electrónica, los "*dark pools*" y las bolsas automatizadas. Los sistemas de operaciones automatizadas y las plataformas de negociación

electrónica pueden ejecutar tareas repetitivas a velocidades muy superiores a las de cualquier equivalente humano. Los controles de riesgo y las salvaguardias tradicionales que se basan en el juicio humano no son apropiados para las operaciones automatizadas, lo que ha provocado problemas como el Flash Crash de 2010. En algunos mercados electrónicos se han establecido nuevos controles, como los frenos a la negociación o los "disyuntores", para hacer frente a los sistemas de operaciones automatizadas.

2.5 Votebot

Un votebot es una automatización de software construida para participar de forma fraudulenta en encuestas en línea, elecciones, y para hacer *upvote* (*like*) y *downvote (dislike)* en las redes sociales.

Los votebots simples son fáciles de escribir y desplegar, al mismo tiempo a menudo son eficaces en muchas encuestas en línea, ya que el desarrollador del software de encuestas debe tener en cuenta este tipo de ataque y hacer un trabajo extra para defenderse de él.

La *World Wide Web* utiliza el protocolo HTTP para transferir información. Los bots de votación están diseñados para imitar el comportamiento legítimo de los usuarios, como votar en una encuesta en línea, interactuando con el servidor que alberga la encuesta mediante el protocolo HTTP. El bot emula así el comportamiento de un humano que utiliza un navegador web, pero puede repetir este comportamiento emulado muchas veces, emitiendo así muchos votos.

En muchos proyectos de votación, los desarrolladores tratan de distinguir los bots de los usuarios legítimos. Por ejemplo, algunos sitios web restringen el número de votos que una dirección IP puede realizar en un periodo de tiempo. Los bots suelen saltarse esta restricción utilizando direcciones IP proxy o VPN. Otros sitios web analizan la cuenta creada por un votebot y su historial de acciones en el sistema para identificar posibles votebots. A su vez, los votebots contrarrestan esto, tratando de simular la actividad humana, como el inicio y el cierre de sesión antes de votar.

YouTube, Facebook, Twitter y Reddit son los principales objetivos de los robots de votación. Muchas personas intentan programar o comprar *scripts* maliciosos para votar por sí mismos en algunos procesos, y es difícil contar el número de ataques que se producen cada día.

2.6 Social bot

Un social bot o algoritmo social, es un agente de software que se comunica de forma autónoma en las redes sociales. Los mensajes (por ejemplo, *tweets*) que distribuye pueden ser simples y operar en grupos y diversas configuraciones con control humano parcial (híbrido) a través del algoritmo. Los bots sociales también pueden utilizar la inteligencia artificial para expresar los mensajes en un diálogo humano más natural.

Los social bots pueden ser utilizados para:

a) proporcionar un agente de atención al cliente de bajo costo para responder a las preguntas que puedan tener sus usuarios.

b) responder automáticamente a las preguntas más frecuentes en medios

sociales como Discord.

c) influir en las decisiones de la gente, por ejemplo: anunciar un producto, apoyar una campaña política, aumentar las estadísticas de participación en las páginas de las redes sociales, etc.

Sin embargo, según Lutz Finger[3], la mayoría de los social bots pertenecen al grupo de los bots disfuncionales (*malicious bots*) porque por lo general son usados para:

- Fomentar la fama: tener un número arbitrario de bots (no revelados) como seguidores (falsos) puede ayudar a simular el éxito real.
- Influencia por encargo: se refiere a la economía que ha surgido en torno a la compra y venta de influencia en las plataformas de medios sociales.
- Seguidores fantasma: son usuarios de las plataformas de medios sociales que permanecen inactivos o no realizan ninguna actividad, pero no participan en los gustos, comentarios, mensajes y publicaciones.
- Spamming: tener bots publicitarios en los chats online es similar al spam por correo electrónico, pero mucho más directo.
- Sesgo de influencia social: que hace que los usuarios compensen en exceso las valoraciones negativas pero amplifiquen las positivas.
- Travesuras: por ejemplo, registrar a un adversario con un montón de identidades falsas y hacer spam en la cuenta o ayudar a otros a descubrirlo para desacreditar al adversario.
- Sesgo de la opinión pública: influir en las tendencias mediante innumerables mensajes de contenido similar con frases diferentes.
- Limitar la libertad de expresión: los mensajes importantes pueden quedar fuera de la vista por un aluvión de mensajes de bots automatizados.
- Suplantación de contraseñas u otros datos personales.

Los Twitter bots son ejemplos ya conocidos, pero también se han observado agentes autónomos correspondientes en Facebook y otros lugares. Hoy en día, los bots sociales están equipados con, o pueden generar, opiniones convincentes en Internet que son capaces de influir en personas reales.

El uso de bots sociales va en contra de las condiciones de servicio de muchas plataformas, como Twitter e Instagram, aunque está permitido en cierta medida por otras, como Reddit y Discord. Incluso para las plataformas de medios sociales que restringen los bots sociales, se pretende, por supuesto, un cierto grado de automatización al poner a disposición las API de los medios sociales. Las plataformas de medios sociales también han desarrollado sus propias herramientas automatizadas para filtrar los mensajes que provienen de bots, aunque no son lo suficientemente avanzadas como para detectar todos los mensajes de bots.

El tema de la regulación legal de los bots sociales es cada vez más urgente para los responsables políticos de muchos países, sin embargo, debido a la dificultad de reconocer los bots sociales y separarlos de la automatización "elegible" a través de las API de los medios sociales, actualmente no está claro

3 Lutz Finger (Feb 17, 2015). "Do Evil - The Business Of Social Media Bots". forbes.com.

cómo se puede hacer y también si se puede aplicar. En cualquier caso, se espera que los bots sociales desempeñen un papel en la futura formación de la opinión pública, actuando de forma autónoma como influyentes incesantes y sin descanso.

2.7 Wikipedia bot

Un Wikipedia bot es una herramienta automatizada que realiza tareas repetitivas y simples para mantener, por ejemplo, las 56.940.456 páginas de la Wikipedia en inglés. Los bots son capaces de realizar ediciones con gran rapidez, pero pueden perturbar la Wikipedia si se diseñan o manejan de forma incorrecta. Por estas razones, se ha desarrollado una política de bots.

Actualmente hay 2.604 tareas de bots aprobadas para su uso en la Wikipedia en inglés; sin embargo, no todas las tareas aprobadas implican la realización activa de ediciones. Los bots dejarán mensajes en las páginas de discusión de los usuarios si la acción que el bot ha llevado a cabo es de interés para ese editor. Algunos bots pueden ser excluidos de dejar estos mensajes utilizando las etiquetas `{{bots}}`. Hay 205 bots que cumplen con la exclusión, que se encuentran en esta categoría. En este momento hay 317 bots marcados con la bandera "bot" (y más de 400 antiguos bots). También hay una serie de herramientas que permiten la edición semiautomática de un gran número de artículos.

2.8 Twitter bot

Un Twitter bot es un tipo de software de bot que controla una cuenta de Twitter a través de la API (interfaz de programación de aplicaciones) ofrecida por Twitter. El software de bot social puede realizar de forma autónoma acciones como tuitear, retuitear, gustar (*like*), seguir, dejar de seguir o enviar mensajes directos a otras cuentas. La automatización de las cuentas de Twitter se rige por un conjunto de reglas de automatización que describen los usos adecuados e inadecuados de la automatización.

El uso adecuado incluye la difusión de información útil, la generación automática de contenido interesante o creativo y la respuesta automática a los usuarios a través de mensajes directos. El uso inadecuado incluye la elusión de los límites de velocidad de la API, la violación de la privacidad de los usuarios, el spam y el *sockpuppeting* (manipular a una persona como si fuera un muñeco de calcetín - *sock puppet* – recurriendo a suplantación de identidad). Los bots de Twitter pueden formar parte de una red de bots más amplia. Pueden utilizarse para influir en las elecciones y en campañas de desinformación.

2.9 Botnets y zombies

La palabra "botnet" proviene de las palabras "robot" y "red". El término suele utilizarse con una connotación negativa o maliciosa. Un botnet es una red o grupo de dispositivos conectados a Internet, cada uno de los cuales ejecuta uno o más bots. Las redes de bots pueden utilizarse para realizar ataques de denegación de servicio distribuidos (DDoS), robar datos, enviar spam y permitir al atacante acceder al dispositivo y a su conexión. El propietario puede controlar la botnet mediante un software de comando y control.

Un botnet es una colección lógica de dispositivos conectados a Internet, como computadores, smartphones o dispositivos del Internet de las cosas (IoT) cuya seguridad ha sido vulnerada y cuyo control ha sido cedido a un tercero. Un dispositivo es comprometido cuando un dispositivo es penetrado por el software de una distribución de *malware* (software malicioso). El controlador (humano) de un botnet es capaz de dirigir las actividades de estos computadores comprometidos a través de canales de comunicación formados por protocolos de red basados en estándares, como el IRC y el Protocolo de Transferencia de Hipertexto (HTTP). Los ciberdelincuentes alquilan cada vez más las redes de bots como mercancía para diversos fines.

En informática, un computador zombi es un computador conectado a Internet que ha sido vulnerado por un hacker, un virus informático o un troyano y que puede ser utilizado para realizar tareas maliciosas bajo dirección remota. Las redes de computadores zombi se utilizan a menudo para difundir spam por correo electrónico y lanzar ataques de denegación de servicio (DDoS). La mayoría de los propietarios de computadores zombi no están conscientes de que su sistema se está utilizando de esta manera. Dado que el propietario del equipo tiende a no estar consciente, estos computadores se comparan metafóricamente con los zombies. Un ataque DDoS coordinado por múltiples máquinas de la red de bots también se asemeja a un ataque de horda de zombis.

Como resultado de la unión de un equipo a un "botnet", a parte de ser utilizados para fines delictivos, los equipos afectados pierden rápidamente recursos informáticos como capacidad del procesador o ancho de banda, ya que éstos son utilizados por los bots instalados en su sistema.

2.10 Chatbot y Test de Turing

Un chatbot o chatterbot es un "*software agent*" utilizado para mantener una conversación de chat en línea a través de texto o de texto a voz, en un lenguaje natural, en lugar de proporcionar contacto directo con un agente humano. De esta forma, empresas o instituciones pueden poner a disposición de sus usuarios interlocutores de ayuda de manera permanente y a bajo costo.

Este tipo de bots es diseñado para simular de forma convincente el modo en que se comportaría un humano como interlocutor. Para lograr aquello los sistemas de chatbot suelen requerir ajustes y pruebas continuas, y muchos de los que están en producción siguen siendo incapaces de conversar adecuadamente. Ciertamente, ninguno de ellos lograría pasar el Test de Turing.

Alan Turing formuló en 1950 una idea sobre cómo determinar si un computador, es decir, una máquina, tenía una capacidad de pensamiento equivalente a la de un ser humano. Él mismo llamó originalmente a esta prueba el *Imitation Game*, que inicialmente era sólo un esbozo teórico. Sólo después de su muerte en 1954 se formuló de forma más precisa y concreta, adquiriendo el nombre de Turing Test, después de que la inteligencia artificial, como subcampo de la informática, se convirtiera en una disciplina académica independiente. Desde entonces, este test ha estado en boca de todos en el debate sobre la inteligencia artificial.

En el test de Turing, un interrogador humano mantiene una conversación con dos interlocutores desconocidos a través de un teclado y una pantalla, sin

contacto visual ni auditivo. Uno de los dos interlocutores es un ser humano, el otro una máquina. Si el interrogador no puede distinguir cuál de los dos es la máquina tras el intenso interrogatorio, la máquina ha superado la prueba de Turing y se supone que tiene una capacidad de pensamiento igual a la de los humanos.

Programas como ELIZA[4] (creado en 1966) han parecido brevemente humanos a los interrogadores humanos en la prueba sin poder pasar formalmente el test de Turing. En su estrategia de respuesta, sólo parecían responder a su contraparte; los sujetos de prueba no eran conscientes de que podían estar tratando con interlocutores no humanos.

En octubre de 2008, un experimento realizado en la Universidad de Reading con seis programas informáticos no alcanzó la marca del 30%. El mejor programa consiguió engañar al 25% de los participantes humanos en el experimento.[5]

En la defensa contra el spam, es necesario distinguir las entradas automatizadas de las que provienen de seres humanos. El método CAPTCHA que se suele utilizar para ello deriva su nombre del test de Turing (*Completely Automated Public Turing test to tell Computers and Humans Apart*). Otro nombre para este método es *Human Interaction Proof* (HIP).

3. De los Social bots en particular

3.1 Descripción

Un social bot es un programa automático que simula el comportamiento humano en las redes sociales. Los bots sociales participan en debates en Twitter o Facebook y actúan como usuarios humanos. Difunden contenidos sobre un tema concreto en las redes sociales, sobre todo con el fin de influir en las opiniones de las personas.

Los bots sociales suelen utilizarse con fines de marketing o políticos. No es raro que los bots sociales difundan noticias falsas. Para influir en la opinión pública, un bot social utiliza técnicas que son típicas de los bots y que también son utilizadas por otros tipos de bots. Buscan en las redes sociales discusiones sobre temas predefinidos e influyen en ellas como participantes en conversaciones virtuales (simulación de conversaciones como con un bot de chat).

3.2 Funciones y funcionamiento

En cuanto a su funcionamiento, los social bots son muy similares a los chat bots o asistentes digitales: se utilizan para comunicarse con las personas. Pero hay una diferencia crucial: mientras que los chat bots suelen ser como un servicio de consultoría, que ayuda al interlocutor, los social bots se supone que engañan y manipulan. Y mientras los chat bots pueden cumplir su función incluso

4 https://www.masswerk.at/elizabot/
5 https://www.telegraph.co.uk/news/earth/3353227/Computers-still-not-quite-clever-enough-to-fool-humans-Turing-Test-shows.html

si son percibidos como programas técnicos, engañar a otros participantes de la red es esencial para que los bots sociales influyan en la opinión pública. Twitter es una de las redes más populares para los social bots, debido a la longitud de los *tweets*/ tuits. Las escasas habilidades lingüísticas de los bots son más difíciles de reconocer en tuits cortos.

Un bot social suele publicar utilizando una cuenta falsa, con su propia foto de perfil, publicaciones y una buena cantidad de seguidores o "amigos". El bot social utiliza esta cuenta para distribuir sus mensajes de marketing o declaraciones políticas. Esto puede hacerse a través de *likes* y *retweets* (re-tuits) o en forma de posts o comentarios. Mediante una interfaz de programación (API), un bot social puede acceder a las redes sociales y recibir y enviar datos.

Los bots sociales suelen operar en momentos en los que otros usuarios están más activos. Además, suelen publicar a intervalos variables para dar la idea de que son humanos cuando en realidad una máquina está detrás de todas las publicaciones.

Un bot social también puede enviar solicitudes de amistad. Si una solicitud es confirmada por un usuario humano, el bot social puede entonces recoger y analizar los datos del usuario. Ya en 2011, un estudio canadiense demostró que los bots sociales son capaces de recopilar datos y analizar la información de la cuenta de los usuarios que han aceptado su solicitud de amistad.

Muchos bots sociales están programados con algoritmos sencillos basados en simples declaraciones "si... entonces…" (if… *then...*): Si se identifica un tema relevante, los bots sociales publicarán el contenido preprogramado. Para encontrar temas relevantes, los bots sociales trabajan con simples búsquedas de palabras clave y escanean las líneas de tiempo de Twitter o las publicaciones de Facebook en busca de palabras y *hashtags* específicos. A continuación, publican textos preescritos como declaraciones o intentan dirigir las conversaciones en una determinada dirección.

Sin embargo, también hay bots sociales que son técnicamente mucho más complejos. Con la ayuda de la inteligencia artificial, el análisis exhaustivo de datos y el análisis de textos, estos bots sociales inteligentes consiguen generar constantemente nuevos comentarios que difieren de los anteriores. A veces, estos bots pueden incluso referirse a los acontecimientos del día. Suelen ensamblar sus *posts* a partir de diferentes textos en línea, que simplemente reordenan. Estos bots sociales más complejos son más difíciles de desenmascarar.

Sin embargo, los bots no funcionan realmente de forma eficiente hasta que están conectados entre sí: Si muchos bots se coordinan entre sí en una llamada red de bots (*botnet*), distribuyen la información de forma aún más eficaz. Por ejemplo, los bots sociales pueden dar "me gusta" y compartir las publicaciones escritas por otros bots sociales. Cuantas más cuentas haya, más crece su influencia.

Para desarrollar un bot social sencillo, no se necesitan conocimientos técnicos especiales: se pueden crear bots sociales sin ningún conocimiento previo de programación, siempre que se utilicen las herramientas adecuadas. Es igual de fácil acceder a cuentas de usuario falsas, ya que se pueden recrear fácilmente utilizando generadores disponibles en línea - o el operador puede simplemente comprar cuentas falsas existentes. Incluso el software de control de estas

cuentas puede comprarse ahora en línea. A través de una interfaz de programación, el bot tiene acceso a Twitter o Facebook, donde reacciona a *hashtags* o palabras clave predefinidas. La tecnología es fácil de conseguir, lo que contribuye a la rápida difusión de los bots sociales.

Sin embargo, la distribución también se ve facilitada por las propias redes sociales, ya que Facebook y Twitter mantienen deliberadamente sus interfaces de programación de acceso (API) relativamente fácil para animar a los desarrolladores de aplicaciones a seguir trabajando en nuevos programas para sus plataformas. Pero esto también significa que los bots sociales no tienen problemas para aprovecharse de ello. Twitter es especialmente fácil de acceder, por lo que la mayoría de los bots se encuentran allí.

En septiembre de 2016, un estudio de la Universidad de Rice estimó que alrededor del 23% de todas las cuentas de Twitter son bots. Esta cifra corresponde a una base global de usuarios activos de aproximadamente 330 millones.[6]

3.3 Los diferentes tipos de social bots

Las funciones básicas de un bot social son siempre las mismas, pero pueden filtrarse en tres categorías según sus funciones: el sobrecargador, el creador de tendencias y el autotroll.

a) El sobrecargador (overloader)

Este es un bot que literalmente inunda una conversación *online* con sus comentarios. Publica las mismas afirmaciones una y otra vez, provocando que los demás mensajes se pierdan de vista. El *overloader* sólo es realmente efectivo si trabaja con otros bots. Cuando una red de bots sobrecarga un *post* con *likes* y comentarios, los usuarios humanos pierden rápidamente el control de la discusión. Esto hace que sea imposible intercambiar contenidos de esta manera.

b) El creador de tendencias

Los creadores de tendencias también funcionan mejor en equipo. Si un gran número de bots sociales se apoderan juntos de un *hashtag*, pueden difundir fácilmente las publicaciones relacionadas con el tema del *hashtag*. Si el tema acaba siendo tendencia en Twitter o Facebook, puede ser recogido por la prensa. De este modo, el bot creador de tendencias distorsiona la relevancia real del área temática elegida. Se aseguran de que fenómenos marginales sean percibidos como tendencias importantes, o pequeños grupos como grandes movimientos sociales.

c) El auto troll

El auto troll opera solo. Intenta distraer a los usuarios que se expresan sobre un determinado tema y trata de involucrarlos en una conversación. Suele hacerlo con declaraciones contradictorias, lo que hace que el usuario tome represalias. Esto distrae al usuario de la conversación original, y la nueva conversación se

6 Why Twitter Is the Best Social Media Platform for Disinformation, en MotherBoard: https://www.vice.com/en/article/bj7vam/why-twitter-is-the-best-social-media-platform-for-disinformation

vuelve polémica y acalorada. Con este método, los bots pueden impedir fácilmente que los usuarios intercambien contenidos.[7]

3.4 Medidas para enfrentar los social bots

Pero también hay medidas que se pueden poner en marcha para limitar lo que pueden hacer los bots sociales. Así, se pueden crear barreras técnicas que impidan o al menos dificulten la creación de cuentas falsas. Una vez determinada la dirección IP de un bot, se puede bloquearlo para que no acceda a la red.

Muchas plataformas utilizan *captchas* para alejar a los bots sociales. Los *captchas* son pruebas cortas que la gente suele pasar sin problemas, pero muchos bots tienen dificultades con ellos. Con un *captcha*, el usuario suele tener que digitar una secuencia de letras alterada gráficamente, que no puede ser leída por una máquina. Sin embargo, cuanto más compleja sea la programación de un bot, mayor será la probabilidad de que sea capaz de resolver *captchas* sencillos.

3.5 Ejemplos de uso de social bots

Hay muchos ejemplos del uso manipulador de los social bots. Solo en 2016 y 2017, se registró el uso de bots sociales en casi todas las elecciones públicas importantes. En particular, hubo amplios debates sobre los bots sociales con respecto a su influencia en la votación del *Brexit* (salida del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea), las elecciones presidenciales en Estados Unidos, así como las elecciones parlamentarias en Francia y Alemania.

La influencia de los bots sociales en el resultado de las elecciones fue objeto de controversia. En particular, se escribió durante meses en la prensa sobre el voto del Brexit y la sorprendente elección de Trump en EEUU. Mucha gente sospechó que los bots sociales se utilizaron como asistentes de voto secreto antes de que se celebraran estas elecciones. Los efectos de los bots sociales y las noticias falsas son evidentes: provocan una gran pérdida de confianza en la comunicación digital.

a) Votaciones del Brexit

En junio de 2016, la mayoría de los ciudadanos británicos decidieron abandonar la Unión Europea (UE). Antes de ello, se produjeron acalorados debates en las redes sociales, y se observó que muchos social bots también participaron. El diario *The Independent* informó de que los bots sociales desempeñaron un importante papel estratégico, especialmente a la hora de votar por el "*leave*" (esp. "salir").

b) Elecciones presidenciales en Estados Unidos

En noviembre de 2016, Donald Trump fue elegido el 58º presidente de los Estados Unidos de América. Hubo mucha información sobre la influencia de los social bots en su estrecha victoria electoral. Según la Universidad de Oxford, los bots automatizados pro-Trump abrumaron los mensajes pro-Clinton. Al parecer, uno de cada tres tuits pro-Trump procedía de un bot. También hubo una noticia

7 Social bots – the technology behind fake news: https://www.ionos.com/digitalguide/online-marketing/social-media/social-bots/

falsa en la que se decía que el Papa había recomendado a Trump para la elección y se compartió casi un millón de veces, incluso por bots sociales. Pero también se registró el uso de bots sociales pro-Clinton.

c) Elecciones parlamentarias alemanas

A la luz de lo ocurrido el año anterior en el Reino Unido, mucha gente estaba preocupada por la posibilidad de que los social bots influyeran en las elecciones federales de 2017. Como resultado, todos los partidos participantes se pronunciaron en contra de su uso en la campaña electoral, aunque los bots sociales no son ilegales en Alemania. Finalmente, no hubo mucha intromisión por parte de los bots de las redes sociales. Sin embargo, debido al número relativamente pequeño de usuarios de Twitter en Alemania, su alcance también fue menor.

d) Encuestas y análisis de redes sociales

Otro efecto de los social bots es que falsean los resultados de los análisis de las redes sociales. Al analizar los "me gusta" y los "retweets", es difícil para los analistas determinar si proceden de cuentas humanas o virtuales. Por tanto, es más difícil determinar la relevancia real de los temas. Esto es una desventaja tanto para las empresas como para los políticos, porque a ambos les gusta basar sus estrategias en los resultados de los análisis de los medios sociales.

3.6 ¿Quién se beneficia de los bots sociales?

Es difícil determinar quién está realmente detrás de un bot social. Hasta ahora, no existe ningún método que pueda identificar con precisión las cuentas falsas. Por lo tanto, es aún más difícil rastrear al operador responsable. Sin embargo, hay aproximadamente cuatro grupos que pueden beneficiarse del uso de bots sociales:

a) Comercializadores/ influenciadores sociales

Empresas pequeñas y grandes pueden utilizar los bots sociales para el marketing encubierto. Como influenciador, se quiere utilizar estos bots para iniciar tendencias e influir en ellas. La información del grupo objetivo también puede obtenerse a través de un bot social, ya que si confirmas la solicitud de amistad de un bot, éste tendrá un acceso completo a los datos almacenados en tu perfil.

b) Figuras u organizaciones políticas

Los grupos de presión o las figuras políticas también son sospechosos de utilizar bots sociales. Por ejemplo, los servicios secretos estadounidenses sospechan que *hackers* rusos estaban detrás de muchas cuentas falsas y bots sociales durante la campaña electoral de Estados Unidos. Sin embargo, no está claro si el ataque provino de delincuentes o del gobierno ruso.

c) Personas interesadas en la formación de la opinión pública

Hay usuarios que quieren influir en la opinión de los demás a través de los bots sociales. Pueden ser individuos, grupos, organizaciones o delincuentes. El tercer grupo -un conjunto de personas difíciles de identificar- es probablemente el más numeroso de los mencionados aquí. Los implicados utilizan los bots para

beneficiar a un partido o para concienciar sobre determinados temas, o simplemente para causar problemas. El objetivo suele ser difundir contenidos de extrema izquierda o derecha. Dado que este grupo es tan heterogéneo, no es tan fácil señalar una intención específica.

d) Los que no tienen intereses reconocibles

Hay una serie de bots sociales relativamente "inofensivos" que, por ejemplo, dejan una cantidad disparatada de *likes* en los comentarios de Star Wars. Los bots de este tipo no sirven a ningún propósito político o económico reconocible. Presumiblemente, a los que están detrás de los bots sólo les gusta "trollear" (molestar) a los demás.

3.7 Efectos y efectividad de los Social bots

Los peligros de los bots sociales radican en que, en la mayoría de los casos, el objetivo de los bots sociales es influir en las opiniones y tendencias en las redes sociales.

> *"La forma más fácil de manipular las redes sociales es aquella en la que los bots sociales producen puro volumen sin generar nuevos contenidos, lo que al principio puede parecer una forma de manipulación relativamente inofensiva, pero sus consecuencias no son insignificantes. A esto se suma el hecho de que las redes sociales están controladas por algoritmos que dan preferencia a los contenidos populares. Las cuentas que tienen muchos seguidores reciben un trato más favorable por parte de la red social y, por tanto, llegan a más usuarios reales."*[8]

Sin embargo, se discute sobre lo bien que los bots sociales llevan a cabo sus tareas. Al fin y al cabo, muchos expertos coinciden en que los bots sociales no hacen muy bien su trabajo y, por tanto, tienen poca influencia en los usuarios de las redes sociales. Un artículo de UX Magazine[9] sostiene que los bots están sobrevalorados, ya que sólo tienen rangos de respuesta limitados y proporcionan respuestas rígidas, lo que los delata.

Existe un consenso sobre la necesidad de investigar más a fondo el trabajo de los bots sociales. Por tanto, cabe suponer que la investigación social proporcionará resultados más precisos en los próximos años. Por razones preventivas, tendría sentido una investigación más detallada de la técnica: Aunque actualmente muchos bots siguen siendo fáciles de desenmascarar, esto no significa que los bots técnicamente avanzados lo sean. Esto aumentaría el potencial de los bots. Por tanto, es necesario desarrollar estrategias de solución en una fase temprana para poder reaccionar ante los avances técnicos.

8 The impact of social bots on elections: https://www.rabbitconsultinggroup.com/single-post/2017/02/06/The-impact-of-social-bots-on-elections

9 Bots are Overrated: https://uxmag.com/articles/bots-are-overrated

3.8 ¿Cómo reconocer un bot social?

Identificar un bot social se ha vuelto mucho más difícil a medida que su complejidad ha aumentado. Sin embargo, hay una serie de preguntas que hacer cuando se trabaja con cuentas de redes sociales para saber si se trata con un humano o no:

a) ¿Qué probabilidad hay de que una persona cree este perfil?

Se trata de obtener pistas a partir de la foto del perfil, la edad de la cuenta o la proporción de seguidores con respecto al número de cuentas que siguen. Esto se debe a que los bots suelen seguir muchas cuentas sin tener ellos mismos muchos seguidores. Si una cuenta sólo tiene dos o tres amigos, la probabilidad de que sea un bot es bastante alta. ¿La foto del perfil parece una instantánea única o una foto de un modelo profesional que el bot podría haber encontrado en cualquier lugar de Internet? La coherencia del texto del perfil también puede indicar si se trata de un usuario humano o no. También se debe comprobar cuándo se creó la cuenta. Muchos bots se desarrollan poco antes de ser utilizados y, por tanto, tienen cuentas bastante recientes.

b) ¿Qué publica la cuenta?

Si la cuenta sigue publicando mensajes similares -con enlaces a los mismos medios o palabras prácticamente idénticas-, es obvio que se trata de un bot que intenta iniciar una conversación sobre un determinado tema. El lenguaje poco natural o los errores gramaticales habituales también sugieren que es obra de un bot. Los bots suelen publicar más de lo que comentan.

c) ¿Con qué frecuencia publica la cuenta y con qué frecuencia le gustan otras publicaciones?

Se puede sacar más conclusiones de la frecuencia con la que una cuenta está activa en las redes sociales. Un número excepcionalmente elevado de publicaciones, de "me gusta" y de "retweets" es tan notable como un número constante de publicaciones al día. También hay que observar el tiempo de reacción de la cuenta: si la cuenta responde y publica apenas unos segundos después, es un claro indicio de que no hay un humano detrás de la cuenta.

d) ¿Cómo responde la cuenta a las preguntas contextuales?

Uno de los métodos más fiables para identificar a un bot es hacer preguntas contextuales. Se trata de preguntas a las que hay que responder de forma diferente según la situación. A los bots sociales les cuesta pensar en el espacio. Si se le pregunta a un bot: "¿Qué aspecto tiene la foto de perfil del usuario que está por encima de ti?", tendrá dificultades para responder a esta pregunta contextual.

e) Recordar los tipos de social bots

Por último, pero no por ello menos importante, siempre tiene sentido recordar cómo funcionan los diferentes bots sociales. Si se tiene enfrente a un 'overloader' o 'auto troll' y con su inquietante comportamiento, es importate no dejarse provocar por él. Incluso si la cuenta no está dirigida por un bot, ayuda a ignorarlo y a discutir constructivamente con otros usuarios. De este modo, se

reduce la influencia de los bots sociales y de los alborotadores humanos.

4. De la magnitud del problema – Un estudio de caso

Investigadores de la Universidad de Adelaida han descubierto[10] una enorme campaña de influencia organizada a favor de Ucrania que ya estaba en marcha en las primeras fases del conflicto armado entre la Federación Rusa y Ucrania. En general, el estudio descubrió que entre el 60 y el 80% de todos los *tweets*/ tuits del conjunto de datos procedían de cuentas de bots automatizados.

Una campaña de propaganda anti-rusa procedente de un "ejército de bots" de cuentas falsas automatizadas de Twitter inundó Internet al principio del conflicto. La investigación muestra que de los más de 5 millones de tuits examinados, el 90,2% (tanto de cuentas bot como no bot) procedían de cuentas pro-ucranianas, mientras que menos del 7% de las cuentas se clasificaban como pro-rusas.

Los datos publicados muestran que hubo una enorme actividad de bots de *hashtags* pro-ucranianos en la primera semana de la guerra. Alrededor de 3,5 millones de tuits con el *hashtag* #IStandWithUkraine fueron enviados por bots en esa primera semana.

De hecho, fue como si alguien hubiera pulsado un interruptor cuando la actividad de los bots pro-ucranianos se disparó de repente al comienzo de la guerra el 24 de Febrero de 2022. En el primer día de la guerra, el *hashtag* #IStandWithUkraine se utilizó en hasta 38.000 tuits por hora, aumentando a 50.000 tuits por hora en el tercer día de la guerra.

En comparación, los datos muestran que casi no hubo actividad de bots pro-rusos entre los principales *hashtags* en la primera semana. En esa primera semana de la invasión, los bots pro-rusos enviaron tuits con los *hashtags* #IStandWithPutin o #IStandWithRussia a un ritmo de apenas unos cientos por hora.

Los expertos en cibernética expresaron su sorpresa por el hecho de que las respuestas rusas en cibernética e Internet fueran tan tímidas. Un investigador del Centro de Estudios de Seguridad de Suiza afirmó: "Las operaciones cibernéticas pro-rusas que hemos visto no sugieren una larga preparación y parecen más bien aleatorias"[11].

El *hashtag* #IStandWithPutin, que parece haber sido ignorado, se originó principalmente a partir de bots automatizados y finalmente se activó una semana después del inicio de la guerra. Este *hashtag* comenzó a aparecer en mayor número el 2 de marzo, el séptimo día de la guerra. En los dos días siguientes, sólo alcanzó los 10.000 tuits por hora en dos ocasiones, muy por detrás de la actividad de los tuits pro-ucranianos.

El uso del *hashtag* #IStandWithRussia fue aún menor, alcanzando sólo 4.000 tuits por hora. Tras sólo dos días de funcionamiento, la actividad de los *hashtags* pro-rusos había desaparecido casi por completo. Los investigadores del estudio

10 Bots manipulate public opinion in Russia-Ukraine conflict, The University of Adelaide: https://www.adelaide.edu.au/newsroom/news/list/2022/09/08/bots-manipulate-public-opinion-in-russia-ukraine-conflict

11 Russia unleashed data-wiper malware on Ukraine, say cyber expert, The Guardian: https://www.theguardian.com/world/2022/feb/24/russia-unleashed-data-wiper-virus-on-ukraine-say-cyber-experts

señalaron que las cuentas de bots automatizados "probablemente utilizados por las autoridades rusas" habían sido "probablemente eliminados por las autoridades ucranianas"[12].

La respuesta a estas cuentas pro-rusas no se hizo esperar. El 5 de marzo, después de que el *hashtag* #IStandWithPutin se pusiera de moda en Twitter, la compañía anunció que había suspendido más de 100 cuentas que habían utilizado el *hashtag* por violar sus "políticas de manipulación de la plataforma y de spam" y por participar en un "comportamiento inauténtico coordinado"[13].

Ese mismo mes, el Servicio de Seguridad de Ucrania (SBU) habría realizado una redada en cinco "granjas de bots" que operaban en el país. Los operadores de bots vinculados a Rusia habrían operado más de 100.000 cuentas falsas en las redes sociales, difundiendo desinformación que "pretendía sembrar el pánico entre las masas ucranianas"[14].

Esta nueva investigación confirma los crecientes temores de que las redes sociales se han convertido en secreto en una "herramienta crítica de guerra de la información que desempeñó un papel importante en el apoyo de occidente a Ucrania", según los investigadores.

Los investigadores de la Universidad de Adelaida se esforzaron por describir las actividades de las cuentas falsas de Twitter de la forma más neutral posible, aunque descubrieron que la gran mayoría -más del 90%- difundían mensajes anti-rusos. Afirmaron: "Ambas partes en el conflicto de Ucrania utilizan el entorno de la información en línea para influir en la dinámica geopolítica y influir en la opinión pública."

Señalaron que los dos bandos implicados en la guerra propagandística tienen cada uno sus propios objetivos y estilo. Los medios de comunicación social rusos impulsan las narrativas sobre sus motivaciones, mientras que los medios de comunicación social ucranianos tienen como objetivo promover y mantener el apoyo externo de los países occidentales y promover sus esfuerzos militares, al tiempo que socavan la percepción de los militares rusos.

Aunque los resultados de la investigación se centraron en los bots automatizados de Twitter, también se encontraron resultados sobre el uso de *hashtags* por parte de tuiteros que no son bots. Hubo un importante flujo de información procedente de cuentas pro-rusas, pero ningún flujo significativo de cuentas pro-ucranianas que no fueran bots.

El bando pro-ucraniano no sólo fue mucho más activo, sino también mucho más avanzado en el uso de bots automatizados. El bando pro-ucraniano utilizó más "*astroturf bots*" que el bando pro-ruso. Los bots *Astroturf* son bots políticos hiperactivos que siguen continuamente a muchas otras cuentas para aumentar el número de seguidores de esa cuenta.

Los investigadores de la Universidad de Adelaida también examinaron el

12 Massive anti-russian 'bot army' exposed by Australian researchers, Declassified Australia: https://declassifiedaus.org/2022/11/03/strongmassive-anti-russian-bot-army-exposed-by-australian-researchers-strong/

13 #IStandWithPutin versus #IStandWithUkraine: The interaction of bots and humans in discussion of the Russia/Ukraine war, Cornell University: https://arxiv.org/abs/2208.07038

14 Australische Forscher decken massive antirussische „Bot-Armee" auf, Overtone-Magazin: https://overton-magazin.de/hintergrund/politik/australische-forscher-decken-massive-antirussische-bot-armee-auf/

impacto psicológico que las cuentas de bots falsos y automatizados tuvieron en las conversaciones en línea durante las primeras semanas de la guerra. Estas conversaciones en un grupo objetivo pueden evolucionar con el tiempo para apoyar u oponerse a gobiernos y políticas, pero también pueden tener un impacto inmediato e influir en las decisiones inmediatas de ese grupo objetivo.

El estudio descubrió que fueron los tuits de las cuentas de bots falsos los que provocaron un mayor "aumento de las conversaciones sobre el miedo" entre el público objetivo. Descubrieron que estas cuentas de bots automatizados "aumentaron el uso de palabras de la categoría miedo, que incluye palabras relacionadas con el miedo y la ansiedad, como 'vergüenza', 'terrorista', 'amenaza', 'pánico'".

Al combinar los mensajes sobre el "miedo" con los mensajes sobre la "mudanza" y las ubicaciones geográficas, los investigadores descubrieron que "las cuentas de los bots influyeron más en las discusiones sobre la mudanza, la huida o la permanencia". Los investigadores creen que este efecto puede haber influido para que los ucranianos huyan de sus hogares incluso fuera de las zonas de conflicto.

La investigación demuestra que las cuentas falsas y automatizadas de los "bots" en las redes sociales manipulan la opinión pública influyendo en el discurso, a veces de forma muy específica. Los resultados proporcionan una indicación escalofriante del impacto maligno muy real que pueden tener las campañas de desinformación en las redes sociales sobre una población civil inocente.

A partir de los idiomas específicos utilizados en los 5 millones de tuits, se pueden deducir algunas pistas sobre el origen y el destino de los mensajes. Más de 3,5 millones de tuits, el 67%, estaban en inglés, y menos del 2% en ruso y ucraniano.

En mayo de 2022, el director de la Agencia de Seguridad Nacional (NSA) y jefe del Mando Cibernético de Estados Unidos, el general Paul Nakasone, reveló que el Mando Cibernético había llevado a cabo operaciones ofensivas de información en apoyo de Ucrania. "Hemos llevado a cabo una serie de operaciones de todo tipo: ofensivas, defensivas y de información"[15], dijo Nakasone.

Desde 2017, los Estados Unidos han invertido 40 millones de dólares para ayudar a Ucrania a fortalecer su sector de tecnologías de la información. Según la Subsecretaria de Estado de EE.UU., Wendy Sherman, las inversiones han ayudado a los ucranianos a "mantener el flujo de Internet y la información, incluso en medio de una brutal invasión rusa"[16].

15 Cyber Command chief confirms US took part in offensive cyber operations, The Hill: https://thehill.com/policy/cybersecurity/3508639-cyber-command-chief-confirms-us-took-part-in-offensive-cyber-operations/

16 US, EU cyber investments in Ukraine pay off amid war, The Hill: https://thehill.com/policy/technology/597921-us-eu-cyber-investments-in-ukraine-pay-off-amid-war/

5. Cambridge Analytica

En este documento hemos puesto, tal como nos fue solicitado, mayor énfasis en los Social bots, pero no queremos dejar pasar esta oportunidad para llamar la atención sobre otros programas/ *scripts*/ *software applications* que permiten un uso malicioso en redes sociales.

En la década de 2010, la consultora británica Cambridge Analytica recopiló datos personales de millones de usuarios de Facebook sin su consentimiento, principalmente para utilizarlos para influenciar procesos electorales mediante publicidad política personalizada y significativa.

Los datos fueron recogidos a través de una aplicación llamada "This Is Your Digital Life" (esp. "Esta es tu vida digital") que consistía en una serie de preguntas para construir perfiles psicológicos de los usuarios. Además, no solo recogía los datos personales de los usuarios de Facebook que habían instalado esta aplicación, sino que recogía los datos personales de los amigos de Facebook de estos usuarios a través de la plataforma Open Graph de Facebook. Si bien, solo unos 270 mil usuarios de Facebook instalaron la aplicación, Facebook estima que los datos personales de unos 87 millones de sus usuarios[17] llegaron a manos de Cambridge Analytica.

Cambridge Analytica utilizó los datos para proporcionar asistencia analítica a las campañas presidenciales de 2016 de Ted Cruz y Donald Trump, y – como revela la importante película documental de la plataforma Netflix "El gran hackeo" ("*The Great Hack*") - de una serie de otros procesos electorales.

La información sobre el uso indebido de datos fue revelada en 2018 por Christopher Wylie[18], un exempleado de Cambridge Analytica, en entrevistas con The Guardian y The New York Times[19]. En respuesta, Facebook se disculpó por su papel en la recolección de datos. En julio de 2019, se anunció que Facebook iba a ser multado con 5.000 millones de dólares por la Comisión Federal de Comercio debido a sus violaciones de la privacidad. En octubre de 2019, Facebook acordó pagar una multa de 500.000 libras a la Oficina del Comisionado de Información del Reino Unido por exponer los datos de sus usuarios a un "grave riesgo de daño". En mayo de 2018, Cambridge Analytica se declaró en bancarrota.

Otras agencias de publicidad llevan años aplicando diversas formas de segmentación psicológica y Facebook había patentado una tecnología similar en 2012. No obstante, la franqueza de Cambridge Analytica sobre sus métodos y el calibre de sus clientes -entre ellos la campaña presidencial de Trump y la campaña *Vote Leave* del Reino Unido- puso de manifiesto los riesgos de la segmentación psicológica contra los que los estudiosos han estado advirtiendo. El escándalo despertó un mayor interés público en la privacidad y la influencia de las redes sociales en la política.

17 https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/
18 https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3
19 https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

El escándalo de los datos de Facebook - Cambridge Analytica recibió cobertura mediática en forma de un documental de Netflix de 2019, "*The Great Hack*"[20]. El documental proporciona información sobre los antecedentes y los acontecimientos relacionados con Cambridge Analytica, Facebook y las elecciones de 2016 que dieron lugar al escándalo de datos en general.

El Grupo SCL era una empresa privada de investigación y comunicación estratégica interesada en estudiar e influir en el comportamiento de las masas. Con una supuesta experiencia en operaciones psicológicas (*psyops*), la empresa trabajó en operaciones militares y políticas en todo el mundo a finales de la década de 1990, incluyendo la campaña electoral en el mundo en desarrollo a lo largo de la década de 2000. Para hacer negocios relacionados con las elecciones estadounidenses, se creó la filial Cambridge Analytica en 2012.

En 2015, Cambridge Analytica, una empresa de consultoría política con sede en el Reino Unido, comenzó a trabajar en nombre de la campaña de Ted Cruz para intentar ganar la nominación republicana en 2016. Utilizó Facebook como medio de "vigilancia político-votante" a través de la recopilación de puntos de datos de los usuarios. Las investigaciones independientes sobre la extracción de datos, junto con los relatos de los denunciantes sobre el impacto de la firma en el Brexit, llevaron a un escándalo sobre la influencia de las redes sociales en las elecciones políticas.

Cambridge Analytica, la empresa responsable del escándalo, se dedicaba al negocio del *big data* (enormes volúmenes de datos, imposibles de ser analizados por humanos). Los datos que se recopilaron estaban destinados a ser utilizados como parte de una estrategia de ventas que implicaba la creación de campañas masivas que se acercaban a los usuarios de manera personal. Los resultados de esta campaña acabaron perturbando la política de EE.UU. y Reino Unido y provocaron denuncias de complicidad de empresas de redes sociales como Facebook.

La recolección ilícita de datos personales por parte de Cambridge Analytica fue denunciada por primera vez en diciembre de 2015 por Harry Davies, periodista de The Guardian. Informó de que Cambridge Analytica trabajaba para el senador estadounidense Ted Cruz y utilizaba datos recogidos de las cuentas de Facebook de millones de personas sin su consentimiento.[21] Siguieron otros informes en la publicación suiza *Das Magazin* de Hannes Grasseger y Mikael Krogerus (diciembre de 2016), (traducido y publicado posteriormente por Vice[22]), Carole Cadwalladr en The Guardian (a partir de febrero de 2017) y Mattathias Schwartz en The Intercept (marzo de 2017). Brittany Kaiser, exdirectora de Desarrollo de Negocios de Cambridge Analytica, reveló que todo lo publicado que involucraba a Cambridge Analytica en la campaña del Brexit y la campaña de Ted Cruz era cierto.

El escándalo llegó a tal punto que incluso Mark Zuckerberg, fundador de Facebook, tuvo que declarar oficialmente ante varias comisiones del Congreso de los Estados Unidos.[23]

20 https://www.netflix.com/cl/title/80117542
21 https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data
22 https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win
23 https://www.theguardian.com/technology/live/2018/apr/11/mark-zuckerberg-testimony-live-updates-house-congress-cambridge-analytica