CENTRO DE
INVESTIGACIONES
SOCIALES

UADE
UNIVERSIDAD ARGENTINA

LA FÁBRICA INVISIBLE DE LA POLÍTICA DIGITAL

Granjas de teléfonos, *bots*, *trolls* e inteligencia artificial: nueva arquitectura de la manipulación en campañas electorales

PRINCIPALES HALLAZGOS

Una **“granja de teléfonos”**, sofisticada pieza de la comunicación digital en Argentina, es un **espacio físico con decenas o cientos de celulares conectados y coordinados para simular interacción humana masiva - likes, comentarios, visualizaciones y posteos -**. Sus objetivos son instalar temas, inflar métricas e influir en el clima de opinión pública.

Argentina fue uno de los primeros países en registrar acciones sistemáticas de manipulación digital mediante cyber troops (grupos organizados, generalmente vinculados con gobiernos o partidos, que operan en redes para influir en la conversación pública)

Desde 2018 el ecosistema digital argentino pasó de una desinformación “artesanal” a un modelo algorítmico automatizado; la inteligencia artificial produce y amplifica mensajes (videos, audios y textos sintéticos).

Durante la campaña presidencial de 2023 se detectaron redes masivas de cuentas falsas gestionadas por empresas de marketing político, orientadas a manipular algoritmos y amplificar candidatos.

En 2025, videos deepfake (videos falsos generado con inteligencia artificial) de Mauricio Macri, Javier Milei, Axel Kicillof y Jorge Taiana circularon en plena campaña y veda electoral; alcanzaron más de 500 mil visualizaciones en algunos casos, con intervención judicial y verificaciones públicas.

Las “granjas de iPhone” representan una nueva modalidad de automatización masiva, basada en dispositivos reales y utilizada para spam, estafas y phishing político (fraude mediante mensajes falsos).

Además de robots, detrás de muchas campañas digitales hay personas organizadas que, junto con inteligencia artificial, trabajan para burlar los filtros y simular apoyo genuino (modelos “semiorgánicos” o híbridos); se trata de usuarios humanos coordinados con software de inteligencia artificial para sortear controles de plataformas.

Existe un mercado informal activo de compra y venta de cuentas falsas, seguidores y bots en WhatsApp y Facebook, que alimenta la manipulación algorítmica y la instalación artificial de agenda (temas más relevantes para la discusión pública).

PRESENTACIÓN

La política argentina abandona el escenario tradicional conformado por actos, debates o conferencias de prensa, **y se libra, cada vez más, en espacios invisibles**: servidores, granjas de dispositivos, grupos cerrados de mensajería y redes coordinadas de cuentas falsas. Allí, la conversación pública puede ser fabricada, amplificada o distorsionada en cuestión de horas.

El presente estudio del Centro de Investigaciones Sociales (CIS) de UADE revela que **Argentina fue uno de los primeros países del mundo en registrar operaciones sistemáticas de manipulación digital**. En 2017, el Oxford Internet Institute ya señalaba la existencia de "ciber-ejércitos" vinculados con actores políticos locales. Desde entonces, el fenómeno continuó y se sofisticó.

¿Quién habla cuando creemos que habla la sociedad?

Si en sus inicios la desinformación era ejecutada por trolls humanos y bots relativamente simples, desde 2018 el ecosistema argentino experimentó una transformación estructural. Hoy predomina un modelo automatizado, en el que **la inteligencia artificial genera contenidos sintéticos - videos, audios, imágenes y textos - capaces de simular con notable realismo a dirigentes políticos**.

El salto cualitativo quedó expuesto en 2025, cuando circularon deepfakes de Mauricio Macri, Javier Milei, Axel Kicillof y Jorge Taiana. Algunos superaron las 500 mil visualizaciones. En plena veda electoral, videos falsos anunciaban renuncias o apoyos inexistentes. **La verificación posterior y la intervención judicial no impidieron que los contenidos impactaran en la conversación pública**.

El fenómeno no se limita a cuentas automatizadas. **Este estudio detecta la coexistencia de modelos híbridos: humanos coordinados mediante bots de Telegram, mercados paralelos de compra de seguidores, click farmers, personas que cobran por generar "me gusta", seguidores o clics falsos**, y "granjas de iPhone" que operan con dispositivos reales para evitar bloqueos. La frontera entre lo orgánico y lo artificial se vuelve cada vez más difusa.

Frente a este escenario, el debate académico permanece abierto. Mientras algunas investigaciones sostienen que los efectos de las fake news pueden ser limitados, otras advierten que **la amplificación coordinada y la microsegmentación algorítmica - uso de algoritmos para dividir al público en grupos muy pequeños y enviar mensajes personalizados según sus datos y comportamientos - pueden incidir en la agenda pública, la polarización y la movilización electoral**. Lo que resulta indiscutible es que la arquitectura de la comunicación política cambió, y lo hizo de manera profunda.

RESUMEN EJECUTIVO

- Argentina figura entre los primeros países con operaciones organizadas de manipulación digital documentadas internacionalmente.
- El ecosistema local evolucionó desde trolls humanos hacia automatización algorítmica con inteligencia artficial generativa.
- La IA permite crear perfiles sintéticos con imágenes y voces generadas por deep learning, difíciles de rastrear.
- En la campaña de 2023 se identificaron redes masivas de cuentas falsas gestionadas profesionalmente.
- En 2025 se registraron al menos cuatro casos de deepfakes políticos durante la campaña y la veda electoral.
- Algunos contenidos falsos superaron las 150 mil y 500 mil visualizaciones antes de ser verificados.
- Existen tres modelos operativos: automatizado puro, híbrido humano-IA y servicios comerciales de venta de interacciones.
- Las granjas de dispositivos utilizan bancos masivos de tarjetas SIM para sortear verificaciones telefónicas.
- Funcionan mercados paralelos en WhatsApp y Facebook donde se compran y venden cuentas, seguidores y bots.
- La literatura académica debate el impacto electoral directo, pero coincide en que estas prácticas afectan la agenda pública y la dinámica de la conversación democrática.

EL ESTUDIO

GRANJAS DE TELÉFONOS, BOTS, TROLLS E IA Y SU IMPACTO EN LA COMUNICACIÓN POLÍTICA

Introducción

En el contexto digital actual, la comunicación se perfila cada vez más como una estrategia política sin precedentes, en la que los contenidos sintéticos, los bots, los trolls y las granjas de teléfonos (físicas y digitales) se reproducen y contribuyen a un escenario atravesado por incertidumbre, manipulación y desinformación. El presente estudio examina cómo las granjas de clics, los bots y los trolls - sumados al uso de la inteligencia artificial (IA) - están reconfigurando las estrategias de comunicación política. Desde 2018, el ecosistema digital argentino ha atravesado una transformación significativa, pasando de una desinformación artesanal -operada por trolls y bots humanos- a un modelo algorítmico automatizado. En este nuevo entorno, la IA generativa no solo amplifica mensajes, sino que también los produce: genera videos, audios y textos sintéticos capaces de influir en la opinión pública.

Glosario y tipologías

Los bots son softwares automatizados que generan contenidos en redes sociales imitando comportamientos humanos, como dar "me gusta", escribir comentarios, retuitear o repostear mensajes, entre otras acciones. Su objetivo fundamental es inflar métricas. En Argentina, su uso se detecta desde 2017 en campañas electorales y crisis políticas (Calvo & Aruguete, 2020).

Pueden clasificarse en bots de chat, que envían mensajes directos a los usuarios, por ejemplo en servicios de atención al cliente; bots de difusión, que publican contenido - noticias o publicidades - de manera automática en redes sociales; bots amplificadores, que aumentan la visibilidad de determinados contenidos o mensajes; bots de seguimiento, que monitorean y recopilan información sobre temas, tendencias o usuarios en redes sociales; bots interactivos, que interactúan con usuarios de manera más compleja simulando conversaciones humanas; bots de influencia, que difunden propaganda política o manipulan la opinión pública; y bots maliciosos, que tienen objetivos perjudiciales vinculados con actividades ilegales, como generar spam, realizar ataques de phishing o propagar malware.

Los trolls son personas cuyo objetivo es difundir mensajes malintencionados, antagónicos u ofensivos contra otras personas, políticos o gobiernos. Pueden hacerlo a través de sus propias cuentas o mediante cuentas falsas. Su finalidad suele ser incidir en la opinión pública o en el estado de ánimo de las personas.

Las granjas de teléfonos físicas son un "ejército" de dispositivos dispuestos en un espacio y coordinados para enviar mensajes de manera sistemática con objetivos específicos, tales como instalar temas y marcas, influir en la opinión pública a favor o en contra de candidatos políticos, entre otras acciones. Las granjas de teléfonos digitales cumplen el mismo propósito, pero sin contar con dispositivos físicos (Maldita.es, 2025).

EL ESTUDIO

Las granjas de bots son redes coordinadas de cuentas automatizadas cuyo objetivo es imitar el comportamiento humano. Estos sistemas suelen utilizarse para manipular métricas digitales, inflar interacciones en redes sociales o propagar desinformación. Debido a las medidas adoptadas por las empresas de redes sociales, estas granjas se han vuelto cada vez más difíciles de detectar y suelen vincularse con estrategias comerciales poco éticas (Santoso & Khan, 2025).

Las granjas de clics surgieron principalmente en el sudeste asiático y en América Latina. Se trata de sistemas de microtrabajo organizado en los que los trabajadores reciben un pago mínimo por realizar clics y así conseguir seguidores para influencers o marcas, o bien para difundir desinformación (Grohmann et al., 2022). Suelen considerarse una forma de marketing online fraudulento basada en una acción comercial ilegítima a través del spam de clics (Lindquist, 2018).

El click flooding es una técnica mediante la cual se generan clics falsos sobre campañas publicitarias con el objetivo de agotar el presupuesto de anunciantes legítimos (SpiderAF, 2024).

El smishing es una forma de phishing que se realiza a través de SMS o servicios de mensajería.

Las cyber troops, o tropas cibernéticas, son grupos organizados -generalmente vinculados a gobiernos o partidos políticos- que operan en el entorno digital para influir en la opinión pública e instalar conversaciones en internet (Bradshaw & Howard, 2017). Estas tropas operan en al menos 80 países y utilizan bots, trolls humanos, influencers pagos, cuentas duplicadas en redes sociales como Instagram, Facebook y X, y plataformas como WhatsApp y Telegram, con objetivos claros y predefinidos de desinformación (OSCE, s. f.).
Los click farmers son personas que trabajan generando interacciones digitales artificiales - como clics, “likes”, visualizaciones, seguidores o comentarios - de manera sistemática y coordinada, generalmente a cambio de un pago.

La manipulación algorítmica refiere a prácticas mediante las cuales las cuentas de bots nacen en espacios cerrados, como grupos de WhatsApp o Facebook, y luego engañan a los sistemas de recomendación para que consideren determinados contenidos como relevantes o de interés público. Asimismo, pueden desplegar estrategias de framing para desprestigiar personas y estrategias de agenda setting que logran instalar temas a partir de señales artificiales.

La opacidad algorítmica se refiere a la dificultad para comprender cómo funcionan los algoritmos y cómo toman decisiones. Esto puede afectar a las personas influyendo en lo que ven o compran, sin que adviertan que están siendo guiadas por algoritmos mediante burbujas de filtro, agenda setting algorítmico o microtargeting.
La gestión algorítmica opaca describe sistemas de control y organización sin transparencia basados en algoritmos que asignan tareas, regulan el rendimiento y distribuyen recompensas y sanciones sin que exista claridad sobre los criterios de decisión ni posibilidad efectiva de apelación.

EL ESTUDIO

Origen de las granjas de teléfonos y bots

El Oxford Internet Institute describió los primeros registros de operaciones de manipulación en redes alrededor de 2010, al revelar la existencia de operaciones político-digitales profesionales destinadas a instalar temas mediante "ciber-ejércitos" de bots y operadores humanos (Bradshaw & Howard, 2017). Las granjas de dispositivos constituyen uno de los tipos de engaño más antiguos (La Nación, 2019). Estas operan en espacios físicos con numerosos dispositivos desde los cuales se generan clics, registros, visualizaciones, impresiones y creación de perfiles falsos, además de reseñas y actividades simuladas para aparentar legitimidad.

Ya en 2012, Facebook buscaba implementar filtros para detectar los "me gusta" creados automáticamente (AdAge, 2012), aunque no lograba identificar aquellos generados de manera coordinada a través de granjas de clics. En 2013, la plataforma estaba inundada de interacciones producidas por trabajadores que cobraban un dólar cada 1.000 "me gusta" (Business Insider, 2013). En Indonesia, uno de los países con mayor uso de redes sociales, se consolidó un mercado global de compra de seguidores y de click farmers, contratados en su mayoría por organizaciones de Norteamérica y Europa (Lindquist, 2018).

A pesar de la escasa información disponible sobre granjas de clics, una de las primeras reportadas fue detectada en Tailandia en junio de 2017, donde se encontraron cientos de teléfonos móviles y miles de tarjetas SIM utilizadas para generar "me gusta" y visualizaciones en WeChat (News.com.au, 2017).

Existen también registros de granjas de clics en América Latina desde 2015, aunque su uso se expandió durante la pandemia. En Brasil, algunas de las principales plataformas son GanharNoInsta, Dizu, FarmarSocial y SigaSocial. En Colombia, una de las plataformas identificadas es SEOsprint (Grohmann et al., 2022).

Si bien las granjas de clics pueden considerarse una forma de trabajo "low tech", forman parte del ecosistema de plataformas de microtrabajo que integran inteligencia artificial. En el informe de Grohmann se señala que, en GanharNoInsta, la asignación de tareas a los trabajadores está automatizada mediante sistemas de gestión algorítmica opaca.

Uno de los pocos testimonios públicos sobre estas prácticas corresponde a Gastón Douek, especialista en campañas políticas digitales, quien en una entrevista a La Nación (2019) afirmó haber armado una maquinaria de trolls en la campaña mexicana de 2012: "Para que te hagas una idea: en un solo día, Twitter nos bajó 48.000 cuentas. Teníamos 150.000 cuentas". Según su relato, la granja estaba totalmente automatizada y no utilizaba trolls humanos. También aclaró que esa escala era posible en otro contexto tecnológico, dado que en los últimos años X (ex Twitter) ha perfeccionado sus mecanismos de detección de cuentas falsas.

EL ESTUDIO

Funcionamiento

Las granjas de teléfonos son instalaciones físicas que concentran una gran cantidad de dispositivos móviles configurados para realizar actividades en línea de manera automatizada. Suelen ubicarse en países con salarios bajos, como China, India o Indonesia, desde donde se activan manual o automáticamente, modificando direcciones IP y utilizando VPN o redes de proxies para evitar su detección (Maldita.es, 2025).

Una de sus principales ventajas es que pueden sortear ciertas barreras impuestas por plataformas como X, Facebook e Instagram, que requieren verificación mediante número telefónico. Esto se logra a través de la adquisición masiva de bancos de tarjetas SIM (Centro de Ciberseguridad de Buenos Aires, 2024).

Recientemente se ha identificado una modalidad denominada "granjas de iPhone", que implica el uso masivo de dispositivos Apple para el envío automatizado de spam, engaños, estafas y phishing mediante iMessage (Forbes Argentina, 2025).

Ante los esfuerzos de las plataformas por frenar la automatización maliciosa, las operaciones de influencia se están desplazando hacia esquemas "semiorgánicos" más complejos, que combinan usuarios humanos coordinados con software de inteligencia artificial (Santoso et al., 2025). Un ejemplo es el uso de bots de Telegram para coordinar miles de personas remuneradas que comparten contenido de manera estratégica.

Según la cuenta Buenos Días Santiago (citada en Balcarce, 2025), pueden identificarse tres modelos operativos. El primero es completamente automatizado, con bots gestionados exclusivamente por software. El segundo es híbrido, en el que grupos de personas administran cuentas automatizadas que generan y difunden contenidos sintéticos. El tercero corresponde a servicios comerciales que venden seguidores, visualizaciones o clics (Balcarce, 2025).

Un elemento central de este ecosistema es la existencia de mercados paralelos e informales en WhatsApp y Facebook, donde se compran y venden cuentas falsas, seguidores y bots (Grohmann et al., 2022). Asimismo, algunos youtubers actúan como "skill makers", funcionando como intermediarios que introducen a personas en el circuito de granjas de clics mediante tutoriales sobre cómo obtener ingresos incrementando seguidores e interacciones (Grohmann et al., 2022).

Granjas de clics, trolls y bots en Argentina

El informe Troops, Trolls and Troublemakers (Bradshaw & Howard, 2017) señala a Argentina como uno de los primeros países en registrar acciones sistemáticas de manipulación en redes sociales. Estas actividades responden principalmente a requerimientos del Estado o de partidos políticos. El informe documenta tanto mensajes de apoyo a gobiernos como interacciones negativas, incluyendo trolling y ataques contra opositores.

EL ESTUDIO

El informe Freedom on the Net 2024 de Freedom House destaca que durante la campaña electoral de 2023 se detectaron redes masivas de cuentas falsas gestionadas por empresas de marketing político, cuyo objetivo era manipular algoritmos para amplificar mensajes y candidatos. También señala un incremento de trolls, especialmente en redes donde figuras políticas y comunidades de seguidores potencian su accionar.

En una entrevista publicada por Alconada Mon en La Nación (2023), Fernando Cerimedo confirmó la utilización de campañas de trolls y bots con el objetivo de "generar más relevancia y mentirle al algoritmo".

Manipulación algorítmica

Las cuentas de bots suelen originarse en espacios cerrados como grupos de WhatsApp o Facebook y, mediante manipulación algorítmica, engañan a los sistemas de recomendación para que consideren determinados contenidos como relevantes o de interés público. A partir de allí, se desarrollan estrategias de framing destinadas al desprestigio personal y estrategias de agenda setting que instalan temas a partir de señales artificiales. Posteriormente, estos contenidos pueden legitimarse mediante cobertura periodística o su circulación por líderes de opinión y cuentas reales.

Transformaciones con IA

Con la expansión de la inteligencia artificial, proliferan perfiles con imágenes sintéticas generadas mediante técnicas de deep learning, lo que facilita la creación de cuentas difíciles de rastrear (DFRLab, 2021; Brookings Institution, 2024). En este contexto, la IA y el Big Data resultan centrales para la generación, circulación y retroalimentación estratégica de contenidos.

Analisis de casos

Como parte de la investigación, se incluyen cuatro casos de candidatos políticos argentinos en los que se utilizó inteligencia artificial para manipular contenidos y amplificar su circulación mediante bots y/o trolls.

Caso 1: Video deepfake de Mauricio Macri (26 de octubre de 2025)

Se difundió en redes un video manipulado con IA que simulaba al expresidente Mauricio Macri anunciando la baja de la candidatura de Silvia Lospennato. Según Forbes Argentina (26 de octubre de 2025), el material fue verificado como falso por Noticias Argentinas y se solicitó su retiro de plataformas digitales. Fue difundido en plena veda electoral desde cuentas afines a La Libertad Avanza.

EL ESTUDIO

Caso 2: Videos manipulados de Javier Milei y Axel Kicillof (7 de septiembre de 2025)

Circularon videos falsos generados con IA. En el caso de Axel Kicillof, el video obtuvo más de 150 mil visualizaciones en X. Chequeado analizó el contenido con la herramienta Hive Moderation y confirmó su manipulación. En el caso de Javier Milei, el video superó las 500 mil visualizaciones y fue difundido como si se tratara de contenido auténtico de campaña.

Caso 3: Video deepfake de Jorge Taiana (26 de octubre de 2025)

Se difundió un video falso en el que Jorge Taiana anunciaba su baja de candidatura. Chequeado (2025) e Infobae (2025) confirmaron que había sido generado mediante clonación de voz e imagen. La Fiscalía Electoral intervino al considerar que el material afectaba la percepción pública en plena veda.

Caso 4: Video de Mauricio Macri llamando a votar por Provincias Unidas (26 de octubre de 2025)

Durante las elecciones legislativas circuló un video falso en el que Mauricio Macri llamaba a votar por el partido Provincias Unidas. Chequeado verificó que se trataba de una falsificación creada con IA. El contenido se difundió masivamente en WhatsApp y X, evidenciando las dificultades actuales de control electoral frente a la generación sintética de mensajes políticos.

Conclusiones

Aunque las campañas políticas disponen de recursos tecnológicos cada vez más sofisticados, existe debate académico sobre su impacto real en la opinión pública y el comportamiento electoral. Desde enfoques de efectos limitados, Guess et al. (2020) sostienen que la exposición a fake news puede tener efectos acotados, más allá de incrementar la creencia en afirmaciones falsas.

En contraste, perspectivas de efectos más robustos argumentan que la desinformación y las campañas coordinadas pueden incidir significativamente en la agenda pública, la polarización y la conducta política. En entornos digitales, la microsegmentación y la amplificación mediante bots y trolls pueden intensificar estos efectos, incluso influyendo en la movilización electoral (Bond et al., 2012). Estudios recientes, como la revisión sistemática de Rodič (2025), señalan que los bots constituyen una de las herramientas tecnológicas más potentes para la manipulación coordinada de la opinión pública con fines políticos.

Para conocer más sobre este informe de investigación elaborado por el Centro de Investigaciones Sociales de UADE: insod@uade.edu.ar

Acceda a nuestros otros informes de investigación:
https://www.uade.edu.ar/sites/investigacion/

FICHA TÉCNICA

Estudio realizado por el Centro de Investigaciones Sociales (CIS), UADE.

Metodología: investigación descriptiva y analítica de carácter cualitativo-documental con análisis de casos.

Fuentes académicas consultadas:

Amnistía Internacional. (2018). El debate público limitado: Trolling y agresiones a la libre expresión de periodistas y defensores de derechos humanos en Twitter Argentina.
Bradshaw, S., & Howard, P. (2017). Troops, trolls and troublemakers: A global inventory of organized social media manipulation. Oxford Internet Institute.
Calvo, E., & Aruguete, N. (2020). Fake news, trolls y otros encantos: Cómo funcionan (para bien y para mal) las redes sociales. Siglo XXI.
Santoso, A. F., & Khan, Z. (2025). The dark side of bot farms in the business world: An ethical and economic threat in the digital era. Bincang Sains Dan Teknologi, 4(3), 101–105.

Fuentes periodísticas consultadas:

Forbes Argentina. (2025). Qué son las granjas de iPhone.
Infobae. (2024). EE.UU. y sus aliados desmantelan una granja de robots rusa impulsada por IA.
Infobae. (2025, 26 de octubre). Circuló un video falso de Jorge Taiana creado con inteligencia artificial en plena veda electoral.
La Nación. (2023). Así funcionan las granjas de trolls que promueven a Javier Milei.
Maldita.es. (2025). Granjas de clics: cómo cientos de móviles generan falsas interacciones.

Objeto de análisis: Granjas de teléfonos (físicas y digitales), granjas de bots y de clics, trolls, cyber troops, manipulación algorítmica e inteligencia artificial aplicada a campañas políticas.

Alcance temporal: evolución del fenómeno desde 2010 a 2025, con énfasis en el período 2018–2025 en Argentina.

Staff

Daniel Sinopoli
Juan Pablo Bolivio
Mercedes Lehmann, docente investigadora de la facultad de Comunicación, UADE.

Vocero: José Crettaz, decano de la Facultad de Comunicación, UADE

UADE