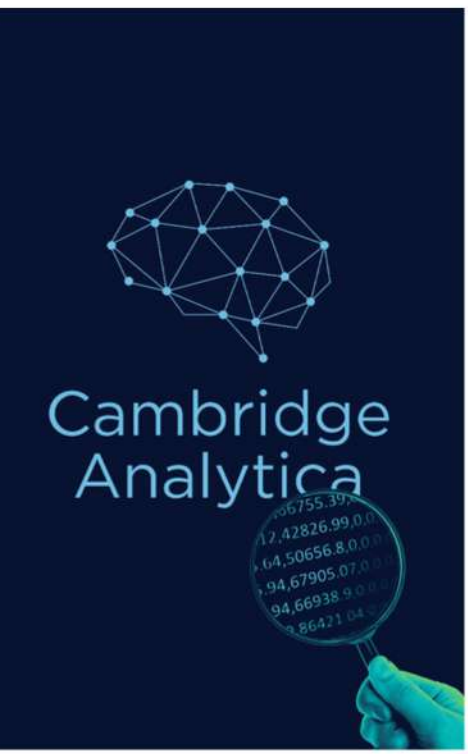
fundaciónHermes
derechos de ciudadanía digital

El microtargeting

Un arma clave para la manipulación electoral



El escándalo de la consultora británica Cambridge Analytica todavía resuena como el paradigma del uso indebido de datos con el propósito de manipular procesos democráticos. Vale la pena recordar el caso por dos buenos motivos: el primero, porque se descubrió el pastel gracias a una denuncia interna y no a una supervisión externa eficiente; y el segundo, porque no afectó a un país con escasos recursos para proteger la intimidad digital de sus ciudadanos, sino a dos grandes potencias como EE UU y Reino Unido. Además, popularizó el uso del microtargeting, una técnica que permite enviar mensajes específicos a grupos pequeños de personas, basándose en su comportamiento y preferencias, lo que fácilmente resulta en **manipulación y desinformación del usuario** con la intención de dirigir su preferencia política.

"Gracias a las redes sociales y la cantidad de datos que se manejan de los perfiles de los usuarios, esta práctica del microtargeting ha sido muy importante en varios contextos", asegura Ignacio Torreblanca director del Consejo Europeo de Relaciones Exteriores (ECFR) y miembro del consejo asesor de la Fundación Hermes. "En algunos casos", añade, "se ha utilizado para lo que en Estados Unidos se llama la supresión del voto: desincentivar o desanimar a votantes potenciales de un rival a que acuda a votar y de esa manera debilitar sus posibilidades de victoria".

Conviene tener presente el caso de **Cambridge Analytica** porque aunque la firma desapareció, sus malas artes no. La crisis estalló en marzo de 2018 cuando un ex empleado de la consultora, Christopher Wylie, reveló que la empresa había accedido a los datos personales de millones de usuarios de Facebook sin su consentimiento para influir en elecciones clave, incluyendo las presidenciales de Estados Unidos en 2016 y el referéndum del Brexit en el Reino Unido. Utilizando una aplicación llamada thisisyourdigitallife, se ofrecía a los usuarios participar en encuestas de personalidad a cambio de pequeños pagos. Al aceptar, también daban acceso a su información en la red social y a la de sus allegados, sin que estos fueran alertados.

¿Acaso esto recuerda al reciente caso de la venta del iris a cambio de criptomonedas en 120 países, incluyendo España? **Cuatro millones de personas vendieron su iris a Worldcoin** antes de que se parara el proyecto.

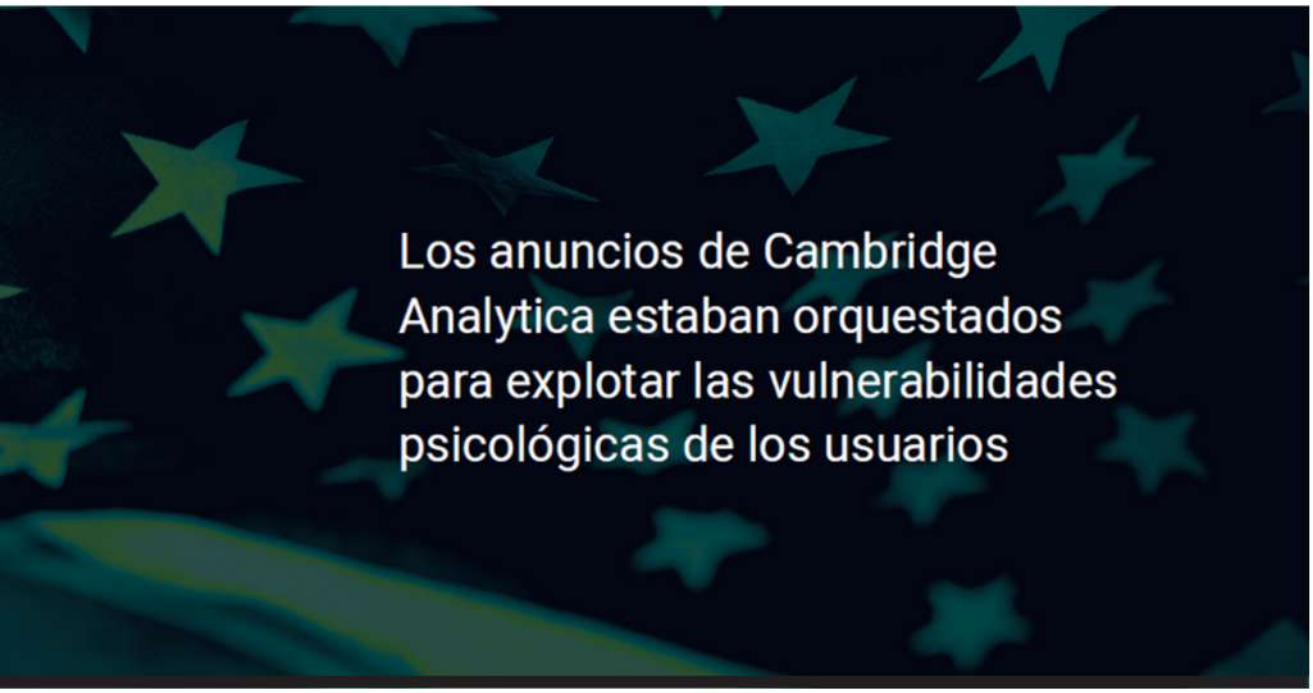
El punto débil del votante

Las víctimas directas de Cambridge Analytica fueron unos 270.000 usuarios –los que se descargaron la aplicación–, pero debido a la estructura de permisos de Facebook en ese momento, la empresa accedió a los datos de aproximadamente 87 millones de personas. La información obtenida incluía **detalles personales, gustos, redes de amistades y más**, permitiendo crear perfiles psicológicos detallados de los usuarios y sus contactos. Con toda esta información, la consultora diseñó y dirigió propaganda política personalizada y

270 mil descargas

87
millones de personas se vieron afectadas

altamente segmentada. Los anuncios estaban orquestados para explotar las vulnerabilidades psicológicas de los usuarios, provocando emociones específicas, como miedo o ira, con el fin de manipular la percepción de los votantes sobre los candidatos y los temas de interés, y así influir en su voto.



"Esto fue en gran parte el objeto de la injerencia rusa en las elecciones del 2016. Porque con todos esos datos y esas conexiones, Cambridge Analytica acabó facilitando el trabajo de esa injerencia, que consistía tanto en mostrar a los votantes demócratas las debilidades de la candidatura de Hillary Clinton, como en socavar esa candidatura", relata el analista y director del ECFR, movilizando también el campo republicano, al distorsionar la candidatura de Clinton como una mucho más radical.

5.000  500

mil libras esterlinas (ICO)

La revelación del escándalo desembocó en múltiples investigaciones por parte de autoridades de protección de datos en el Reino Unido, Estados Unidos y otros países. Cambridge Analytica se declaró en quiebra y **Facebook fue multada con 5.000 millones de dólares** por la Comisión Federal de Comercio (FTC) estadounidense y con 500.000 libras esterlinas por parte de la Oficina del Comisionado de Información (ICO) británica, la multa máxima bajo la legislación anterior al Reglamento General de Protección de Datos (GDPR) europeo.

La reputación de la empresa fundada por Mark Zuckerberg sufrió un duro golpe, tanto que, aparte de implementar cambios significativos en su política de privacidad –restringiendo el acceso de aplicaciones de terceros a los datos de los usuarios y mejorando la transparencia sobre el uso de la información personal–, acabó cambiando de nombre para llamarse Meta.

Puerta trasera para manipular elecciones

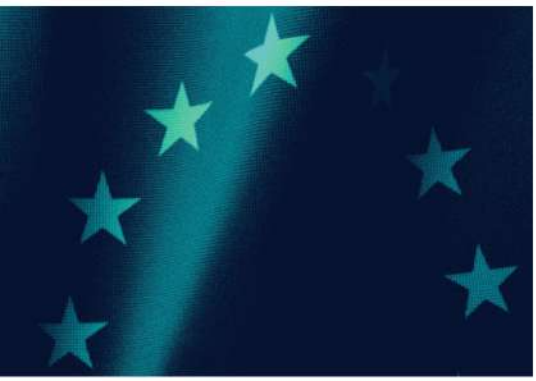
Zuckerberg pidió muchas disculpas tras el escándalo, pero siguió avanzando en la técnica de **microtargeting**, potenciada con la ayuda de la inteligencia artificial, para vender infinidad de productos y servicios. Cookies, rastreadores y otras tecnologías de seguimiento se utilizan para recabar información sobre el comportamiento de los usuarios y construir perfiles que pueden ser vendidos o usados para fines políticos. "Por un lado, internamente se usan para la polarización, pero por otro, que realmente me parece muy importante, es que ha sido y es una avenida para la influencia extranjera sobre los procesos electorales", advierte Torreblanca.

Aunque la propaganda electoral es legítima, ésta es fácilmente manipulable para incluir la **difusión de noticias falsas o distorsionadas** que condicionan la opinión pública. Ignacio destaca los pasos importantes tomados por la UE en cuanto a la regulación de estas plataformas: "Empezó a hacerlo muy rápidamente después del 2018 con los códigos de conducta, en los que ha estado trabajando con las plataformas para ir eliminando y delimitando la publicidad electoral, de tal manera que se sepa siempre quién está financiando, cómo lo está haciendo, y que se puedan evitar esos efectos distorsionadores".

A lo largo de la legislatura 2019-2024, el Parlamento Europeo alertó sobre los intentos sistemáticos de actores extranjeros de inmiscuirse en las elecciones. Ya en 2019, los eurodiputados observaron un fuerte aumento de la propaganda rusa y de los esfuerzos por eludir las restricciones a la financiación extranjera de los partidos políticos. Aparte de la actividad de hackers rusos, **preocupa la injerencia de otros países como Qatar y Marruecos**. Contra esto, los eurodiputados aprobaron una serie de leyes como la de Servicios Digitales, que incluye obligaciones para que las plataformas online luchen contra la desinformación y garanticen un entorno transparente y seguro para los usuarios.

> Aparte de la actividad de hackers rusos, preocupa la injerencia de otros países como Qatar y Marruecos

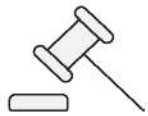
"La UE es pionera en la regulación de estas plataformas, en contraposición a Estados Unidos donde las cuestiones sobre la libertad de expresión tienen una regulación completamente distinta. En Europa están muy bien regulados los delitos de odio, como otro tipo de delitos, que no se amparan bajo una supuesta libertad de expresión. Esto se ha hecho por consenso de las grandes fuerzas parlamentarias y ofrece una defensa mucho más robusta de lo que vemos en otros países", dijo Ignacio.



Las **nuevas normas de transparencia** de la publicidad política prohíben patrocinar anuncios provenientes de fuera de la UE antes de las elecciones. Además, la primera normativa integral del mundo sobre inteligencia artificial (IA) en la UE protege los derechos fundamentales y contrarresta la desinformación al introducir requisitos de transparencia para los contenidos generados por IA.

Europa, en defensa de los periodistas

El Parlamento también adoptó nuevas normas para defender a los periodistas de demandas abusivas y reforzó las disposiciones para proteger la libertad de los medios de comunicación de las injerencias políticas. De hecho, a pesar de los intentos de denigrar el proceso electoral o confundir a los electores en los comicios europeos del pasado 9 de junio, los sistemas de ciberseguridad conjunta de la UE lograron neutralizar el grueso de unas campañas de desinformación cada vez más sofisticadas y potenciadas con herramientas que van **desde la inteligencia artificial hasta páginas web clonadas** de medios de comunicación consolidados.

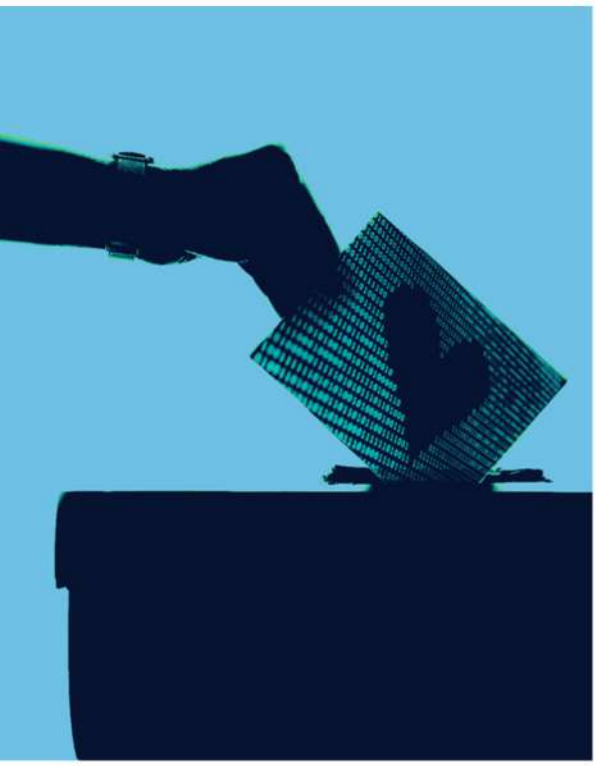


Art. 58 bis

Ley Orgánica 5/1985 (LOREG)

En España, el artículo 58 bis de la Ley Orgánica 5/1985, del Régimen Electoral General (LOREG) regula el tratamiento de datos personales relacionados con opiniones políticas y el envío de propaganda electoral por medios electrónicos. Si bien la LOREG establece la necesidad de **obtener el permiso expreso de los ciudadanos** para el tratamiento de sus datos, existe preocupación sobre la forma en que se obtiene dicho consentimiento. Algunos críticos afirman que en muchos casos el visto bueno se solicita de manera poco clara o se obtiene a través de prácticas manipuladoras, lo que limita el verdadero control de los individuos sobre sus datos.

"Hemos visto que, gracias a estos instrumentos legislativos y gracias a esta conciencia sobre la situación, la UE puede abrir procedimientos de infracción contra estas plataformas por su interferencia", destacó Ignacio.



El uso de datos personales para fines políticos plantea un **dilema ético** sobre la privacidad de los individuos. Por un lado, los partidos políticos argumentan que necesitan acceder a estos datos para adaptar sus mensajes a las preferencias de los votantes. Por otro lado, los defensores de la privacidad sostienen que esto puede vulnerar los derechos individuales y abrir la puerta a la manipulación. Porque, si bien la normativa otorga a los partidos políticos el derecho de utilizar datos personales relacionados procedentes del censo electoral u otras fuentes accesibles al público, el consentimiento expreso es fundamental para que los partidos políticos puedan tratar tus datos personales.

Los votantes tienen garantizados una serie de derechos que pueden ejercer en relación con el tratamiento de sus datos personales. Entre ellos están saber cuáles se recopilan y para qué, consentir o no su tratamiento por parte de los partidos políticos, acceder, rectificar, suprimir y/u oponerse al uso de sus datos personales por parte de los partidos políticos. En caso de que el ciudadano sienta que sus datos personales están siendo utilizados de manera inapropiada, **puede presentar una reclamación ante la Agencia Española de Protección de Datos** o comunicarse directamente con el partido político responsable para que tomen medidas al respecto. Pueden ponerse muchos cortafuegos legales y tecnológicos para impedir la propaganda y manipulación política malintencionada, pero es la educación y la información de los ciudadanos a la hora de protegerse de los abusos en la era digital la mejor arma para salvaguardar sus derechos de privacidad.

Sponsors

Colaboradores