Se remonta a ese momento de su creación, Zuckerberg ante el teclado tras tomar unas copas, creando una página para comparar la apariencia de la gente, sin otra razón más allá de que podía hacerlo. Ese es el aspecto crucial de Facebook, el elemento principal que no se entiende de su motivación: hace las cosas porque puede. Zuckerberg sabe cómo hacer algo, y otra gente no, así que lo hace. Ese tipo de motivación no funciona en la versión de la vida que ofrece Hollywood, y Aaron Sorkin tuvo que dar a Zuck un motivo relacionado con las aspiraciones sociales y el rechazo. Pero eso es incorrecto, totalmente incorrecto. No lo motiva ese tipo de psicología doméstica. Lo hace porque puede, y las justificaciones sobre "conexión" y "comunidad" son racionalizaciones ex post facto. El impulso es simple y más básico. Por eso el impulso para el crecimiento ha sido fundamental para la compañía, que en muchos aspectos se parece más a un virus que a una empresa. Crece, multiplica y monetiza. ¿Por qué? No hay razón. Porque sí.

La automatización y la inteligencia artificial tendrán un gran impacto en todo tipo de mundos. Estas tecnologías son nuevas y reales y vendrán pronto. Facebook está profundamente interesado en esas tendencias. No sabemos hacia dónde va, no sabemos cuáles serán los costes y consecuencias sociales, el próximo modelo de negocio que resulte destruido, la próxima compañía que tome la senda que siguió Polaroid, la próxima industria que siga el camino del periodismo o el próximo juego de herramientas y técnicas que estén disponibles para la gente que utilizó Facebook para manipular las elecciones de 2016. No sabemos qué vendrá a continuación, pero sabemos que probablemente tendrá consecuencias, y que una parte importante tendrá que ver con la mayor red social del planeta. Sobre la base de las acciones de Facebook hasta ahora, es imposible afrontar esta perspectiva sin inquietud. –

Traducción del inglés de Daniel Gascón.
Publicado originalmente en London Review of Books.

JOHN LANCHESTER es escritor. Sus libros más recientes son la novela *Capital* (2013) y el ensayo *Cómo hablar de dinero* (2015), ambos en Anagrama.

GOLPE AL SUEÑO DEMOCRÁTICO

MARTA PEIRANO

Hasta finales de marzo, casi todo el mundo pensaba que la vigilancia tenía que ver con dos cosas: terrorismo y publicidad. Y no les parecía tan grave. Qué más me da que me vigilen si es para enseñarme anuncios de cosas que me interesan. Qué me importa si no tengo nada que ocultar. A finales de marzo, un canadiense de veintinueve años con gafas de pasta y el pelo rosa introdujo una variable que muchos no habían considerado: la vigilancia blanda también puede servir para destruir la democracia. O, al menos, para conseguir que un número suficiente de ciudadanos apoye decisiones colectivas que van en detrimento de la sociedad. Según Christopher Wylie, Cambridge Analytica usó los datos personales de cientos de millones de personas para intervenir con éxito los resultados de al menos dos procesos democráticos. Primero, ganaron el Brexit. Con ese triunfo, se constituyeron como empresa con el dinero de Robert Mercer, una de las dos grandes fortunas detrás de la campaña de Donald Trump. La otra era Peter Thiel, el hombre detrás de Palantir.

Según explicó Wylie ante la comisión del parlamento británico, todo empieza con un test titulado "This is your digital life". Diseñado por el catedrático de psicología de Cambridge Aleksandr Kogan, estaba basado en el popular modelo OCEAN, que hace una evaluación de la personalidad basado en cinco rasgos principales: Openness (apertura a nuevas experiencias), Conscientiousness (responsabilidad), Extraversión, Amabilidad y Neuroticismo o inestabilidad emocional. El modelo es popular porque mide características que trascienden a las culturas, modas y localismos. Funciona igual en Almería que en Alaska, hace veinte años que dentro de seis.

En un principio, Kogan colgó el test en dos plataformas que facilitaban micropagos a los usuarios: el Turco mecánico de Amazon y Qualtrics, una empresa de estudios de mercado. El test tenía ciento veinte preguntas, y ofrecen entre dos y cuatro dólares por completarlo. La cosa no despega hasta que lo sube a Facebook, donde los *quiz* están de rabiosa actualidad.

Kogan encuentra a 270.000 personas dispuestas a completar el test. Los términos de usuario dicen: "Si pinchas ok, nos das permiso para diseminar, transferir o vender tus datos". Nadie lo lee. Además de conceder acceso indiscriminado a todos los datos asociados a su cuenta, incluyendo información sobre su estado civil o su orientación religiosa, también ofrecen acceso a los datos de todos sus amigos. Esto le vino muy bien al proyecto: aunque Kogan dijo que el test era para estudiar el uso de emoticonos para expresar emociones, en realidad estaba diseñado para construir un algoritmo predictivo de patrones psicológicos. Facebook les dio las dos bases de datos que necesitaban para hacerlo, un *dataset* con la característica específica que quieres predecir (*feature set*) y otro con las variables sobre las personas para las que quieres predecirlo (*targets* variables).

Antes de seguir, un detalle. Facebook ha acusado a Kogan y CA de romper el acuerdo de desarrolladores que firmaron cuando subieron la *app* al sistema. El acuerdo dice que los datos de los usuarios no se pueden comercializar. Solo que el acuerdo también dice que audita y vigila todas las aplicaciones para asegurarse de que cumplen las condiciones necesarias, y el *quiz* estuvo allí año y medio hasta que el propio Kogan lo sacó. De hecho, usar *quizzes* para aspirar los datos de los usuarios de Facebook y de sus amigos era una práctica conocida desde al menos 2009, cuando varias asociaciones de defensa de los derechos civiles lo denunciaron. Kogan subió su *quiz* en 2012.

Es más, tres años más tarde Facebook renovó su API, que es la herramienta que intermedia entre los desarrolladores de *apps* externas y la plataforma, y la diseñó de manera que se pudiera seguir haciendo eso. Y más cosas. Kogan tuvo acceso a los mensajes privados de los usuarios. Esto, como dicen los programadores, no es un *bug* sino un *feature*. Facebook sacaba un 30% de todas las operaciones sin preguntar para qué eran los datos ni quién los barría. Facebook calcula que hay 78 millones de afectados, una media de 300 por cada persona que hizo el test. Pero Cambridge Analytica es solo uno de los cientos de miles de agentes que aprovecharon la posibilidad, a costa de la privacidad de miles de millones de personas.

CÓMO GANAR UN VOTANTE

Sería exagerado decir que con un test de personalidad se pueden hackear las elecciones del país más poderoso del mundo. El plan era más complejo y más sensato que eso. No se trataba de manipular a todo el electorado (200 millones de personas) para que votara a Trump, sino hacer un modelo del electorado con 4.000-5.000 *datapoints* (incluyendo el test, pero muchas más cosas) para encontrar a 2-5 millones de personas con un grado alto de neurosis. Los neuróticos son particularmente susceptibles a las teorías de la conspiración. Usarían el algoritmo predictivo para encontrar a los ciudadanos más vulnerables y explotar una vulnerabilidad muy concreta: miedo a los pobres, odio a los negros, ansiedad medioambiental, rechazo a las vacunas, paranoia. Una vez localizado este segmento, lo bombardearían con una campaña de desinformación.

Las campañas de desinformación son anteriores a la red, pero internet las ha transformado en una lucrativa industria de servicios. Una vez localizado su objetivo, Cambridge Analytica no tenía por qué mancharse las manos con las sucias tácticas del gremio. Las podía contratar.

La reina absoluta del *marketing* político es Facebook. No solo está diseñada para extraer la mayor cantidad posible de información sobre sus 2.200 millones de usuarios. La cara B de su negocio es su plataforma de *microtargeting*, que te permite seleccionar cuidadosamente a tus objetivos, dependiendo de su vulnerabilidad. Solo en 2016, *Propublica* descubrió que Facebook tenía habilitado el sistema para segmentar neonazis, supremacistas blancos y revisionistas del Holocausto para campañas específicas. Un poco antes había sido denunciado por vender paquetes de adolescentes con problemas de autoestima a una empresa de cosméticos.

Después están las agencias de noticias falsas, que son como agencias de verdad pero diseñadas para producir contrainformación, desinformación o, simplemente, generar ruido, caos o desastre en torno a un acontecimiento, empresa, persona o producto. La más famosa es la oficina de Macedonia cuyos grandes éxitos incluyen que Obama no era ciudadano estadounidense (y que originó el hilarante movimiento que le exigía mostrar su certificado de nacimiento) y que el papa Francisco apoyaba a Donald Trump (aún hoy una de las noticias más pinchadas de la historia de internet). "Uno podía hacer

creer a la gente las más fantásticas patrañas y confiar en que, si al día siguiente recibía la prueba irrefutable de su falsedad, la misma gente se refugiaría en el cinismo", explicaba Hannah Arendt en *Los orígenes del totalitarismo*. "En lugar de abandonar a los líderes que les habían mentido, asegurarían que siempre habían creído que tal declaración era una mentira, y admirarían a los líderes por su habilidad táctica superior."

Además de Facebook y Twitter, las plataformas favoritas de las agencias de desinformación han sido Instagram y YouTube. Y no siempre les ha hecho falta producir noticias. En un contexto de redacciones mermadas, sobreexplotadas y vendidas a la carrera por el *pagerank*, el contenido viral y el titular pinchable, a menudo solo necesitaban colocarlas de manera estratégica. La campaña de Trump envió a los demócratas afroamericanos un vídeo de Clinton en los noventa hablando de negros. El mensaje: la sucesora de Obama no solo no es negra, sino que está más lejos de Black Lives Matter que del Ku Klux Klan.

Finalmente, entre las agencias de *trolls*, la más famosa es la Internet Research Agency (IRA), vinculada a Putin y con sede en San Petersburgo, pero las hay en China, Venezuela, Indonesia, México, Puerto Rico. Su táctica habitual es activar un enjambre de *cyborgs*, que son cientos de cuentas en las redes controladas por un humano, a las redes sociales. Son básicamente *callcenters*, trabajan por encargo y la clave es el volumen; lo mismo te comentan un producto que te destruyen un rival.

Las nuevas campañas de *marketing* político activan todos esos recursos para crear una especie de meteorología en torno a un tema, partido o candidato. A diferencia de la tradicional, basada en *banners*, marquesinas y mítines, la clave es que no tiene forma de propaganda, tiene forma de información. Envuelve a la gente seleccionada por su vulnerabilidad específica con múltiples contenidos en múltiples plataformas que crean una realidad alternativa. Un filtro burbuja que no tiene nada de voluntario o accidental. Y, aunque no tenemos suficientes datos para saber si es o no es efectiva, sabemos que podría serlo. Y que primero ganó el Brexit, y después Trump.

HACKEAR UNAS ELECCIONES

La táctica era conocida. Mucho tiempo antes de que estallara el escándalo, los dos expertos en seguridad electoral de la Universidad de Michigan J. Alex Halderman y Mathew Bernhard explicaron que la manera más fácil de ganar las elecciones no era tratar de convencer a todos los votantes, sino invertir todos los recursos en el lugar donde más peso tienen.

Hay tres maneras de hackear unas elecciones. Se puede impedir el voto, por ejemplo, con un ataque de denegación de servicio que generaría colas interminables de gente que no puede votar. O impedir que se cuenten los votos. Las dos cosas pasaron en Ucrania en 2012. También se puede contaminar el juego produciendo información que arruine las posibilidades del candidato que no nos gusta. Por ejemplo, publicar los correos del Partido Demócrata en los que se ve que Clinton conspiró para quitarle las primarias a Bernie Sanders. Esta es una muy buena jugada porque le quita votos de su propia gente, no de la tuya.

Finalmente, se pueden alterar los resultados electorales. Naturalmente, el sistema está diseñado para que sea muy difícil. Para hacerlo de manera mecánica, habría que alterar el resultado. Hacerlo con votos de papel es prácticamente imposible, pero EEUU usa máquinas de votar. Técnicamente, las máquinas no están conectadas a la red pero están programadas por máquinas que sí lo están. Si transmiten un *malware* que altera el resultado, se podría hacer. Es muy difícil, pero no imposible. Halderman y Bernhard pensaban en hackear las máquinas, pero su estrategia era la misma que Cambridge Analytica: no tiene sentido hackearlas todas, solamente las que necesitas para ganar. Encuentra los estados donde la diferencia entre los dos candidatos está debajo del 1% y/o los más relevantes por representación (típicamente: Michigan, Pensilvania, Florida y Wisconsin). Después encuentra en el proceso a las compañías de servicios informáticos contratadas con menos recursos y ataca solo ahí. Esas compañías son los neuróticos de Cambridge Analytica, la estrategia es la misma. Wylie dijo que su *conversion rate* era de entre un 5-7%.

El test de Kogan fue solo el principio del proyecto, necesitaban más bases de datos. Para conseguirlos, Cambridge Analytica debutó en la campaña de Ted Cruz. Allí recaudaron la base de datos de los votantes que Facebook no podía darles, una estrategia brillante de Robert Mercer. Desde entonces ha apoyado financieramente todo tipo de causas republicanas, siempre con la condición de que Cambridge Analytica entre en el paquete, quedándose con todos los datos necesarios para alimentar, testar y refinar sus algoritmos. Entre Cambridge Analytica –ahora refundada en Emerdata– y Palantir, Donald Trump tiene a su servicio los dos algoritmos de predicción del comportamiento más poderosos del planeta. Donald Trump volverá a presentarse a las elecciones dentro de dos años. Peter Thiel ya ha dicho que va a mudarse a Los Ángeles para empezar un imperio mediático. Es difícil saber quién es más peligroso. Ni cómo detenerlos ahora que ya están aquí. –

Este texto fue presentado en el 4º Congreso de Periodismo Cultural, organizado por la Fundación Santillana, el Ayuntamiento de Santander y el Centro Botín.

MARTA PEIRANO es periodista especializada en tecnología. En 2015 publicó *Pequeño libro rojo del activista en la red* (Roca).