Internet del comportamiento

Qué es cómo podría influir en la Seguridad Nacional

Rogelio Villajos Rodríguez
Teniente del EA

–Hay que saber cuándo se es conquistado.
–¿Tú lo sabrías? ¿Y yo?[1]

¿Hemos sido conscientes del desembarco de los conquistadores? ¿De todas las infraestructuras construidas para explotar nuestras tierras, ahora convertidas en sus nuevos territorios?

Evidentemente no, pues entraron en nuestras vidas hace veinte años y es ahora cuando comenzamos a ser mínimamente conscientes de ello.

Hasta marzo del año 2000, momento en el que estalla la llamada burbuja financiera de las empresas punto-com, el objetivo de las nuevas empresas que nacían para desarrollar su negocio en internet era crecer, crecer muy deprisa, para una vez alcanzado un tamaño que asegurara su liderazgo en un mercado, pensar en cómo hacer rentable la empresa explotando su dimensión y situación de monopolio.

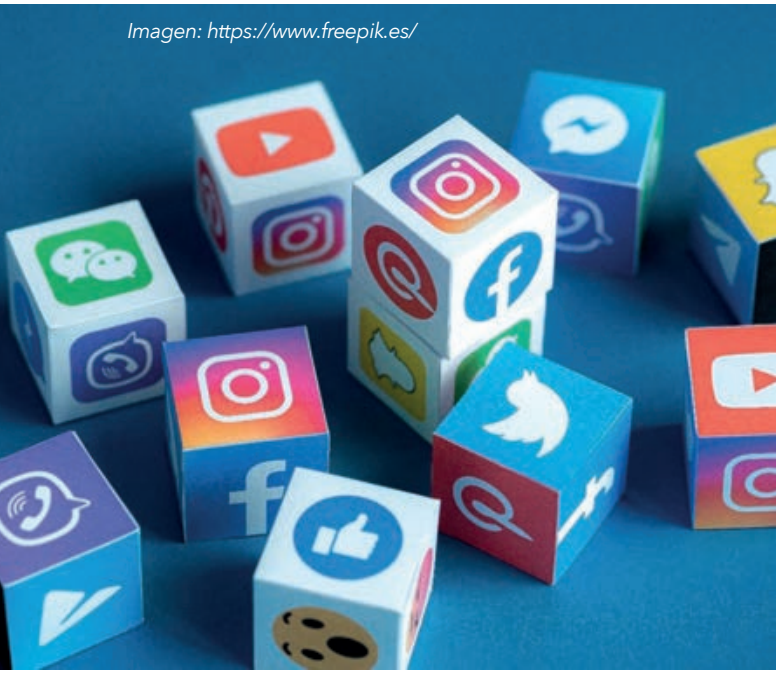


Imagen: https://www.freepik.es/

Tras esta crisis, que provocó una caída en año y medio del 78 % de la capitalización bursátil del Nasdaq, las nuevas empresas tecnológicas llamadas a sí mismas del conocimiento, seguían buscando la forma de hacer rentable su modelo de negocio. Fue en ese momento de necesidad cuando los ingenieros de Google tuvieron una idea que les permitiría monetizar su actividad. Fueron conscientes de la cantidad de información que podían obtener sobre una persona simplemente observando sus historiales de búsquedas. No necesitaban un *software* demasiado avanzado para inferir que alguien que buscara cada semana agencias de viajes, era alguien que se desplazaba con relativa frecuencia.

Siguiendo ese razonamiento, si conseguían información suficiente como para distinguir qué podría desear comprar ese usuario, podrían subastar entre los vendedores de ese producto esa posible compra potencial. En 2003 Google patenta Generating User Information for Use in Targeted Advertising[2], un sistema que les permite relacionar todas las búsquedas con la información aportada como usuario (esos campos solicitados para registrarnos que incluyen nombre, dirección…) y deducir un perfil básico de este, para así, poder seleccionar la publicidad más relevante y con mayor posibilidad de rentabilización.

Los beneficios de Google se dispararon, pasando de 400 millones de dólares en 2002, a 3200 millones en 2004, se habían multiplicado por ocho en solo dos años[3].

Entendiendo que esta era la senda de la rentabilidad, Google se lanza a la conquista de todos los posibles rasgos conductuales que pudiera dejar un usuario en la red. Servicio gratuito de correo electrónico, suite ofimática en red, google-maps, sistema de alojamiento de archivos en servidores, traductor, zoom… todos estos servicios tienen un solo objetivo: parametrizar el comportamiento humano, tanto a nivel individual como

Imagen: https://www.freepik.es/

colectivo, utilizando cualquier posible rastro que pueda dejarse en su uso. Y es que el valor monetario de las subastas sobre posibles compras futuras de los usuarios excede con creces el coste de los servicios prestados y las aplicaciones desarrolladas. No somos conscientes de que con cada recarga de página aparece nueva publicidad, con cada *scroll* aparece nueva publicidad, al ver el correo, o leer el periódico…

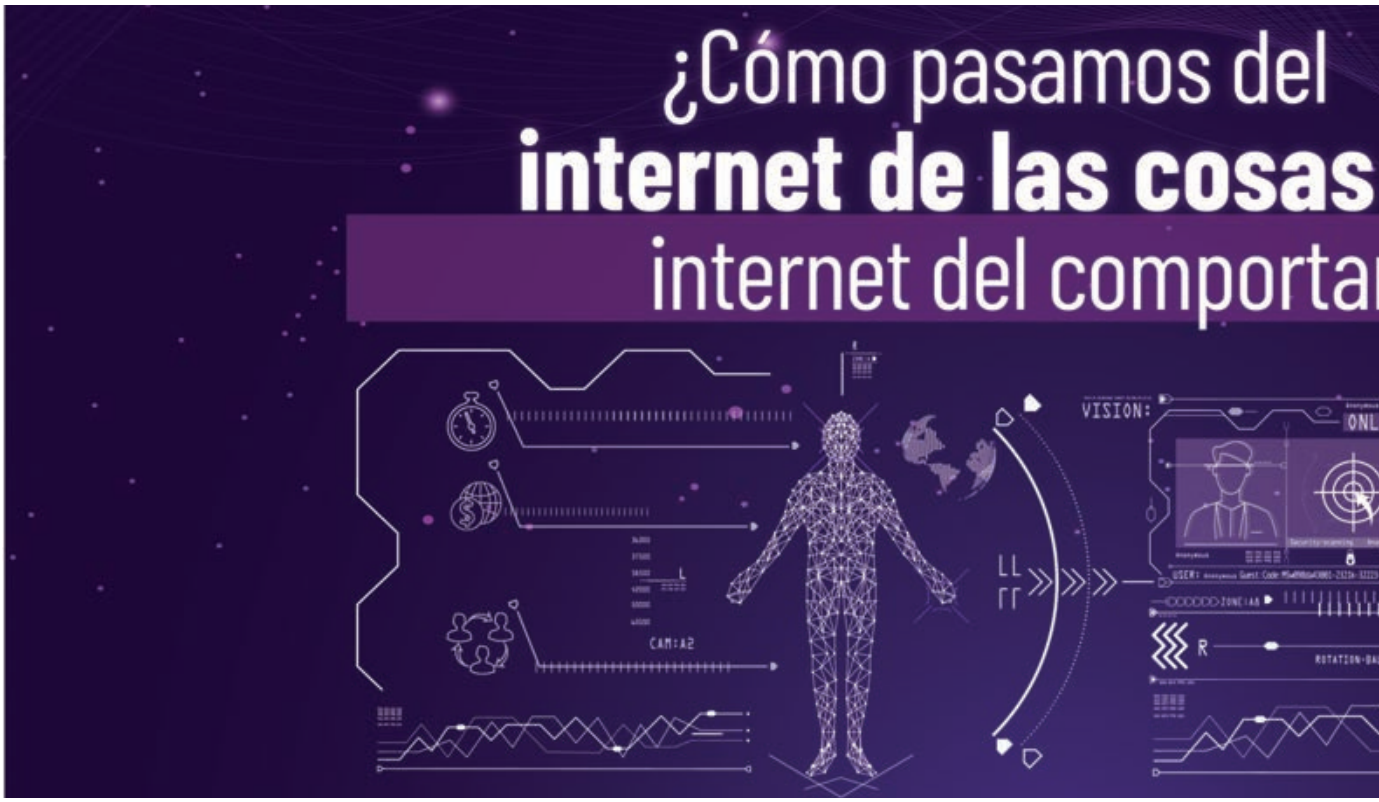
Otras grandes empresas se han sumado a la explotación de la experiencia humana, como Facebook (a la que pertenecen WhatsApp e Instagram), Twitter, Amazon, Microsoft, Apple… y proporcionar datos a estas que completen y perfeccionen los perfiles de los usuarios, es el negocio principal de muchas otras (todas las apps gratuitas del móvil; juegos, reproductores, herramientas…).

Para conseguir algoritmos que se perfeccionen y consigan buenas predicciones sobre nuestro comportamiento futuro se necesita una cantidad ingente de datos con dos características; que sean diversos, es decir, que recojan experiencias diversas como patrones de voz, rutinas de actividad física, gustos estéticos, relaciones personales… y que sean cientos, de miles, de millones de datos, para poder afinar sus patrones estadísticos.

Este *software* avanzado ejecuta de forma constante pruebas A/B complejas sobre la población de usuarios.

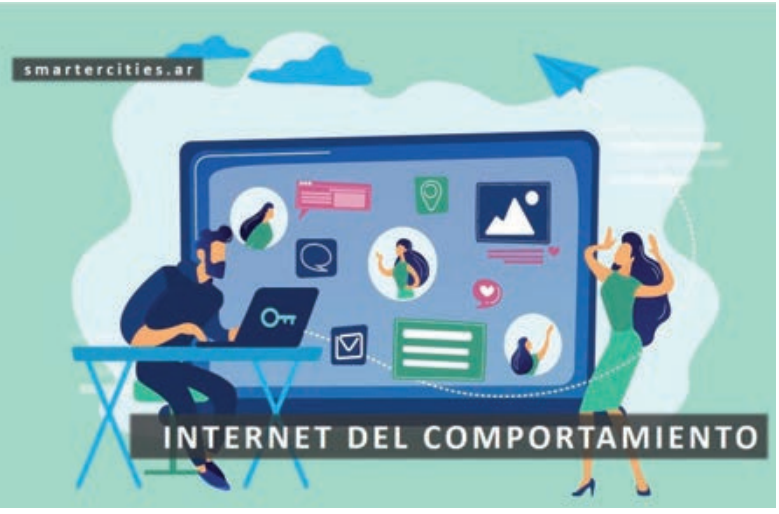
Imagine que es usted ese *software* buscando el aumento de tiempo del usuario en su red. Divide a su población en dos grupos, el A, al que no realiza ninguna prueba, y el B, al que modifica algún parámetro observable y cuantificable,

Imagen: https://wwwhatsnew.com/



como subir un tono el color de fondo de una página web. Al finalizar la prueba, mide el tiempo de permanencia en su red de ambas mitades poblacionales, y en función de los resultados vuelve a realizar el test con otros parámetros y otras divisiones poblacionales, siguiendo siempre la senda de los mejores resultados estadísticos.

La recogida de datos que necesitan estos algoritmos se realiza a través de las aplicaciones que descargamos en nuestros teléfonos móviles, de las redes sociales que utilizamos, de los *wereables* que portamos (como pulseras de medición de actividad física o relojes inteligentes), del uso de sistemas operativos y la navegación a través de ordenadores y tablets, y cualquier otro dispositivo con capacidad para recolectar datos y conectarse a internet (como los robots de cocina, nuevos juguetes para niños, barredoras automáticas…), y a través de las llamadas cookies zombi de estos dispositivos.



Al menos tres compañías monitorizan y registran todas nuestras comunicaciones, sean llamadas de voz, emails, mensajes en redes sociales, o comunicación entre objetos (Internet of Things -IoT) en o a través de nuestra red. Toda nuestra comunicación es explotada para la generación de nuestros perfiles de conducta futura por: la compañía telefónica que nos presta el servicio, la compañía que ensambla el dispositivo, y la creadora del sistema operativo que soporta la comunicación. Estas tres compañías son las dueñas del código que denominamos cookies zombi[4] de segunda generación, llamadas de forma eufemística capa de personalización, que monitorizan todo los sensores del dispositivo[5].

La comunicación monitorizada y registrada, independientemente de que en ella estén involucrados humanos, animales o dispositivos electrónicos, se trata de la siguiente forma:

Imagen: https://www.unisabana.edu.co/

• Se extraen de ella todos los datos posibles, y se analizan mediante *software* que interpreta que puede ser útil de ella. El resto se almacena para un posible uso futuro. Todas las posibles inferencias que de sus conversaciones se puedan hacer, ya se están haciendo. Con suficientes datos, de su voz se puede deducir, estado de ánimo, salud, educación, capacidad adquisitiva, su nivel de socialización, posición social y trabajo.

• A través de los análisis realizados, de los cientos de millones que se realizan cada hora, se exploran nuevas formas de detección de experiencia conductual, si es posible lanzar un nuevo dispositivo o aplicación que capte algún rasgo de nuestra experiencia vital que aún no esté siendo explotado. De las conversaciones sobre texto se extraen datos, de las realizadas sobre voz más, y al realizarlas sobre soporte de vídeo se obtiene mucha más información aún, al poder aunar expresiones faciales a lo que se está expresando, lo que permite, además de la creación de perfiles de conducta más ajustados, entrenar las IA con datos de mayor calidad.

• Con los datos se perfecciona la parametrización de la persona, personalizando el proceso de extracción sobre esta misma persona, y permitiendo una acción con mayor probabilidad de éxito sobre él, con lo que el valor monetario sobre las pujas por su conducta futura aumentan.

• La IA que monitoriza el proceso, para optimizar su aprendizaje, hace previsiones constantes sobre esa comunicación, ajustando sus algoritmos en función de la desviación de esas previsiones sobre el resultado final.

Debo volver a recordar que el grueso de los beneficios de estas empresas proviene de la subasta de nuestros comportamientos futuros, inicialmente comportamientos futuros de compra, pero también han sido utilizados para la venta de perfiles a empresas interesadas en ellos, desde cazatalentos hasta aseguradoras, pasando por agencias de seguridad nacional.

Estas empresas pronto comprendieron que los comportamientos inesperados o no predecibles suponían pérdidas, llegando a la conclusión de que la mejor forma de acertar en una predicción sobre el futuro es construir ese futuro. La experiencia humana se ha vuelto de esta forma, no solo medible, parametrizable y predecible, ahora también es modificable.

Para conseguir una influencia tal sobre un sujeto que consiga modificar su conducta, de forma que el propio sujeto no sea consciente de estar siendo manipulado, y logrando que ejecute acciones alejadas del curso normal de acontecimientos en caso de no intervención, se necesitan herramientas capaces de interpretar y descifrar quienes somos completamente.

Para esto, siguiendo las teorías de B. F. Skinner sobre el condicionamiento conductual y la aplicación a través de la tecnología de éstas por parte de Alex Pentland, durante la última década se ha desarrollado la computación afectiva.


Imagen: https://www.giztab.com/

Esta tecnología realiza análisis de emociones y sentimientos, buscando patrones, formas de alteración de esos patrones, y por supuesto, formas de rentabilizar ese conocimiento. Empresas como RealEyes ofertan sus servicios de reconocimiento expresivo facial en tiempo real, con el que se puede conocer el impacto real emotivo de un discurso mientras se está dando, permitiendo su modificación sobre la marcha. O Emoshape, que entrena su IA para modificar, a través de la conversación, el estado anímico y proporcionar uno superior en felicidad a cualquier persona expuesta a su interacción.

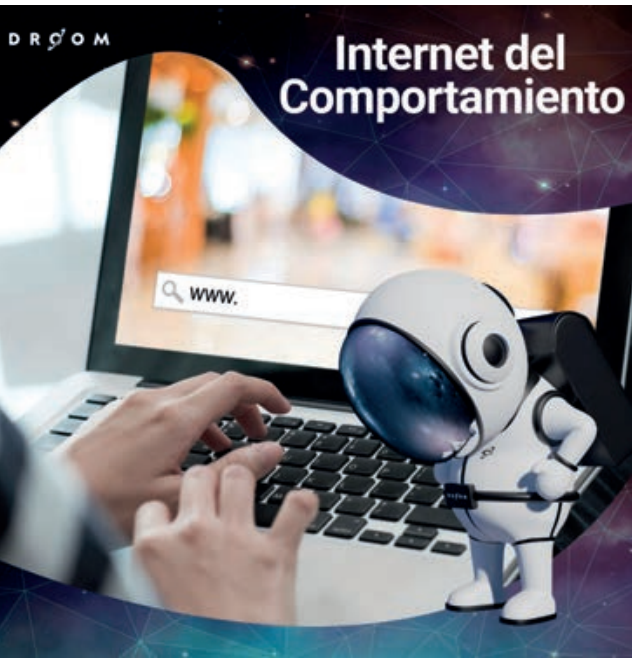
Este es el poder del Internet del Comportamiento (Internet of Behaviors – IoB), su capacidad para conocer nuestra física emocional y vital para poder pilotarnos a voluntad. Se ha necesitado la fusión de tecnologías digitales que permitan la captación de los datos, de las tecnologías basadas en análisis estadístico y machine learning, y de ciencias sociales que estudian el comportamiento humano para conseguirlo.

Y si somos manipulables, pudiendo elegir alguien por nosotros por donde circular, qué comer, a quien votar, qué pensar, a quien amar… ¿qué nos queda? Como comenzaba este artículo, las empresas tecnológicas están esquilmando nuestra naturaleza humana, la han conquistado, eliminando lo que hasta ahora llamábamos libre albedrío.

Existen numerosas razones por las que no podemos desconectarnos de estas empresas: la angustia emocional que nos genera la desconexión social, no pertenecer a grupos y estar enterados de las corrientes sociales, de aquello de lo que se habla. Las repercusiones laborales al romper con las nuevas formas de comunicación entre jefes y subordinados que emplean los medios digitales, ¿cómo renunciar a la inmediatez de los mensajes de whatsapp y su despersonalización que evita la tensión mental del cara a cara? El deseo permanente de disponer de nuevos dispositivos, su vinculación con el estatus social favorecido por la industria…

En los últimos años, se ha estado trabajando en el desarrollo de una doctrina de carácter militar para lo que se ha denominado el ámbito cognitivo. Aunque la forma de enfocar este nuevo ámbito en las operaciones varía entre lo publicado por la normativa OTAN y lo desarrollado por España, conceptualmente se refieren a los mismos problemas y aportan las mismas soluciones.

Imagen: https://blog.sherpa.ai/



Su perspectiva está basada en la visión tradicional de la propaganda de guerra y las operaciones de desinformación, alimentadas en la actualidad por las redes sociales y sus algoritmos, que ofrecen al usuario aquellos contenidos que lo mantendrán más tiempo frente a la pantalla, siendo su contenido usualmente más radicalizado. El desarrollo de esta doctrina está más que justificado por la situación actual, pero no incluye las nuevas amenazas que presenta el IoB.

La doctrina se refiere a las capacidades de influencia que las empresas desarrollaron hace una década, y que ahora están en manos de estados para su uso no comercial. De la misma forma, la creación de gemelos digitales[6] humanos que permite el IoB y que está en manos de empresas a día de hoy, lo estará muy pronto en manos de los estados.

Una vez parametrizada una persona, se puede generar su gemelo digital y someterlo a miles de simulaciones variando parámetros hasta encontrar el curso de acción y/o estímulos necesarios para que esa persona piense, haga o desee lo que se tenga como objetivo que piense, haga o desee.

Los jóvenes militares que nos rodean en las tres escalas (y los que están por entrar), un uso intensivo de las redes sociales (Whatsapp, Instagram, Tik-Tok…), de las wereables de monitorización corporal (pulseras fit, smartwatchs…), y de otra cantidad importante de dispositivos y *software* que los monitoriza de forma ubicua y permanente.

Probablemente se debería comenzar a tomar medidas para evitar que se generen, y en caso de que así sea, que se puedan proteger, los gemelos digitales de nuestros futuros jefes de unidad y estado mayor.

¿Deberían considerarse esta invasión relevante para la Seguridad Nacional? Si entendemos por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, garantizar la defensa de España y sus principios y valores constitucionales[7], la posible modificación en pro de los intereses ajenos de nuestros deseos, opiniones, pensamientos, sentimientos… ¿no impide nuestra libertad? ¿no corre peligro nuestro sistema de principios y valores? ■

NOTAS

[1]Diálogo inicial de la película Gladiator de Ridley Scott.

[2]Generación de Información de usuario para su uso en publicidad dirigida, puede consultarse en: https://patents.google.com/patent/US20050131762A1/en

[3]En 2020 han declarado ingresos superiores a la 180 000 millones de dólares.

[4]Dado que muchos usuarios rechazaban las cookies, o las eliminaban de forma regular, las compañías de seguimiento conductual crearon un código similar al de las cookies habituales pero que se escondía en el dispositivo, de tal forma que no podía ser localizado y podía seguir monitorizando al usuario. Asignaba un identificador único al usuario, independientemente de las cuentas que utilizara. No obstante, podían llegar a localizarse y eliminarlas. Son las cookies zombi de primera generación. Las referidas en el texto no pueden eliminarse, y vienen preinstaladas.

[5]Entre los más habituales están: acelerómetro, sensor de huellas, de proximidad, capacitivos en pantalla, giroscopio, magnómetro, gps, de luz ambiental…

[6]Un gemelo digital en una réplica de un objeto real en un plano virtual. Replicando todos los parámetros físicos de una pieza en un motor, se puede experimentar con ella sin los costes asociados a hacerlo de forma real. Con suficientes datos, ese gemelo digital puede ser un humano.

[7]Página 14 de la Estrategia de Seguridad Nacional 2017.

Imagen: https://www.tendencias21.es