

## THE CONVERSATION

Rigor académico, oficio periodístico



Diego Cervo/Shutterstock

### ¿Qué sabe de usted su robot aspirador?

19 enero 2020 22:04 CET

Durante los últimos años, uno de los productos más vendidos durante las jornadas de rebajas conocidas como *Black Friday* o *Cyber Monday* ha sido el robot aspirador. Sus avanzadas prestaciones, que permiten su puesta en marcha y funcionamiento cuando el usuario está ausente de su domicilio, han seducido de forma clara a los compradores.

Pero este éxito de ventas ha venido acompañado también de algunas dudas: ¿están estos robots adquiriendo datos sensibles que pueden ser vendidos en el mercado global de los datos personales?

#### ¿Qué tipo de datos recogen Roomba y compañía?

El robot aspirador ha sido el primer caso de éxito de la robótica en el ámbito doméstico. En 2002 se fabricó la primera serie de robots Roomba, formada por 15 000 unidades, que se vendió en unas pocas semanas. 18 años más tarde se han vendido millones de unidades y los robots aspiradores representan una importante cuota de mercado en el sector de la limpieza.

Estos agentes electrónicos han evolucionado en distintas direcciones, desde la incorporación de nuevas prestaciones como la capacidad de fregar suelos a la mejora de su “comportamiento inteligente”. Hoy en día disponen de sofisticados sistemas de navegación que les permiten volver a su base de carga en caso necesario y también optimizar la limpieza de una planta entera.

#### Autor

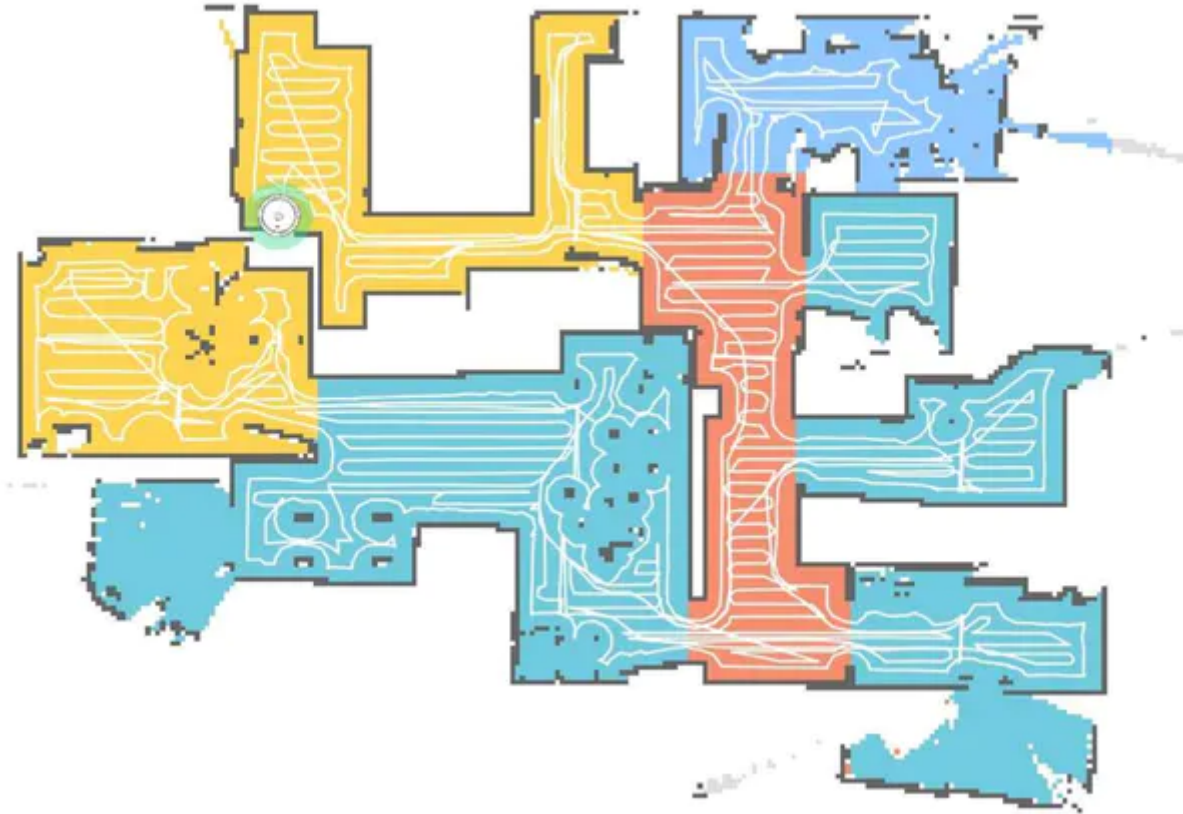


**Jordi Vitrià**

Catedrático de Informática, Universitat de Barcelona

Pero más allá de la guerra de precios y del aumento de sus prestaciones, los robots domésticos han sido protagonistas en los últimos tiempos de alguna polémica relacionada con los datos que recogen sus sensores.

La mayoría de estos aparatos son capaces de usar los sensores para construir un mapa del espacio que deben limpiar y en el caso de los más sofisticados, utilizar cámaras que les permiten identificar obstáculos diversos. Estos mapas pueden ser consultados por los usuarios desde sus móviles usando la aplicación correspondiente.



Mapa creado por un robot doméstico de limpieza. Jordi Vitrià/Flickr, CC BY-NC-SA

No es pues ningún secreto que la incorporación a nuestro entorno doméstico de robots semiautónomos conlleva un nivel de captación de datos muy avanzados: mapas de nuestra vivienda, imágenes, registros de temperatura y humedad, registros horarios, etc.

El anuncio en 2017 por parte del fabricante de Roomba de la posible compartición de algunos de estos datos generó una primera polémica, aún no cerrada, sobre el derecho a la privacidad en el ámbito doméstico. ¿Debemos aceptar que se compartan datos sobre nuestra vivienda? ¿Qué límites se deben imponer? ¿Qué mecanismos tenemos para ejercer nuestros derechos?

La privacidad será, al menos durante la primera mitad del siglo XXI, una de las fuentes de conflicto en un mundo donde la captación de datos personales se ha simplificado extraordinariamente y en el que el cruce de diversas fuentes de datos permite crear perfiles muy precisos de los ciudadanos.

Las ventajas que aportará la digitalización y la robotización de nuestro entorno deberán ser **analizadas críticamente** para no caer en modelos que facilitan la **manipulación social** por parte de los grandes agregadores de datos.

### ¿Cómo se entiende la privacidad en este caso?

La privacidad se puede definir como la capacidad de modular y controlar el acceso de terceros a nuestra información personal. No es un concepto simple. Para ejercer esta capacidad hacen falta herramientas y protocolos.

En el caso que nos ocupa, la captación de datos de nuestra vivienda se debería efectuar con una serie de requerimientos mínimos por parte de los fabricantes:

- El primero, el compromiso por defecto de no compartir ni vender estos datos a terceros sin el consentimiento expreso del usuario, preservando su intimidad, usando una estrategia que se ha llamado *privacy by design*.
- En el caso de solicitar el consentimiento, hacerlo de forma **transparente**. La transparencia se refiere a definir de forma muy clara las intenciones de la demanda y el uso previsto de los datos: no es lo mismo ceder estos datos para que el fabricante mejore el producto en el marco de un proceso interno que venderlos a un tercero que los podrá usar para fines desconocidos.
- Por último, hace falta poner a disposición del cliente mecanismos efectivos para ejercer sus derechos. La empresa debe hacerse **responsable** del uso y consecuencias de la tecnología que utiliza.

### ¿Deberíamos estar preocupados?

Aunque los datos personales que usa una aspiradora robotizada puedan parecer inocuos, su combinación con otras fuentes de datos, también inocuos cuando son considerados de forma independiente, tienen un alto valor para algunas empresas por su capacidad predictiva y también de manipulación, como han demostrado los últimos escándalos alrededor de Cambridge Analytica.

No hay ninguna prueba de que se haya producido ninguna fuga de datos relacionados con los robots aspiradores hasta el día de hoy. Incluso podemos afirmar que algunas empresas han avanzado en la implementación de los requerimientos de privacidad, pero el tema no está cerrado y hace falta mantener el foco sobre él.

Por una parte, la falta de una regulación que vaya más allá de la **normativa europea de protección de datos** hace difícil controlar el comportamientos de nuevas empresas en este ámbito con fuertes presiones para ampliar su cuota de mercado.

Por otra parte, **estudios independientes** parecen indicar que los datos de algunas aspiradoras robóticas son transmitidos a países con una legislación excesivamente laxa respecto a la privacidad.



**Carl Miller**  
@carljackmiller

Our investigation into personal data aired on [@BBCClick](#) this weekend. One of its most important parts is about how a wave of Internet-enabled devices are beaming data out of our homes and to servers across the world.

Here's a vacuum cleaner, beaming a floor plan to China.



348 11:35 AM - May 28, 2019

[338 people are talking about this](#)

Si queremos mantener nuestra preocupación a niveles moderados hace falta una doble acción: dar soporte a las iniciativas de monitorización pública de cualquier elemento con capacidad de captura de información personal y también promover nuevas iniciativas legislativas que apoderen al ciudadano ante esta nueva realidad.



**¿Es buena idea compartir fotos de nuestros hijos en las redes sociales?**

**Datos geolocalizados, la moneda de la geotecnología**

## **¿Por qué nos espían los asistentes virtuales?**

### **La protección de datos, un asunto profundamente humano**