

MI 'YO' DIGITAL: LO BUENO, LO MALO Y LO IMPREVISIBLE

Por: Esteve Almirall, Ulises Cortés. 22/08/2021

La (desorbitada) actividad digital nos lleva a fusionarnos, cada vez más, con la tecnología que utilizamos a diario. Reconocimiento facial, huellas dactilares... ¿Cuáles serán las consecuencias de transportar nuestra identidad hacia lo informatizado?

¿No sería fantástico olvidarse, de una vez por todas, de los contraseñas? En cierta forma, ya está ocurriendo. Cuando nos identificamos con un *smartphone* o a través en la banca *online* no necesitamos ninguna clave. Simplemente miramos a la pantalla y accedemos. **Nuestra identidad digital es nuestro rostro, nosotros mismos.**

Las identidades digitales permiten que las personas se identifiquen de manera segura, fácil y rápida al realizar, por ejemplo, una compra o comenzar un nuevo trabajo sin el tiempo, el esfuerzo y el gasto que implica el uso de un documento físico. Sin embargo, **hay otras identidades digitales menos reguladas** –quizás, de forma natural, menos regulables– que las personas crean con su huella digital, compuesta por todas y cada una de las interacciones que llevamos a cabo a diario con el mundo *online*. Esto incluye redes sociales, *apps*, teléfonos, coches conectados, elementos del Internet de las Cosas y un largo etcétera. En no pocos momentos podemos estar conectados de forma simultánea desde varios dispositivos que están transmitiendo por numerosas bandas de comunicación como el 5G, el *wifi*, el *bluetooth* y el resto del espectro de las comunicaciones móviles.

En nuestra identidad pública queda esa parte que se nos ha robado en las redes sociales y plataformas de compras

Es en este tipo de identidades más informales donde se da, a la vez, el mayor grado de innovación; lo que lleva a toparse con dos fenómenos que crecen con rapidez. Por un lado, el uso de factores biométricos, ya centrado en el reconocimiento facial; por otro, plataformas que facilitan la identificación a aplicaciones de terceros,

convirtiéndose de esta forma en **una autoridad digital de autenticación**. Ambos se entrelazan aportando evidentes ventajas a los usuarios pero también atentan, al menos en Europa, contra la necesaria protección de la privacidad de los individuos.

A medida que se amplía –de manera desorbitada– nuestra huella digital, también lo hace nuestro ‘yo’ digital. Una parte de este es pública, pero solo representa la punta del iceberg –lo que queremos mostrar en las redes (o lo que se comparte sin nuestro consentimiento expreso)–. **Oculto queda esa proporción que se nos ha robado sin darnos cuenta**, la que pertenece a las redes sociales, plataformas de compras y aquellas compañías que pagan por esta información.

De la misma manera que la sociedad se basa en la construcción colectiva de la realidad, el espacio virtual de las sociedades digitales –que abarca mucho más que la *web*– abre nuevas oportunidades de interacción y negocio. Las redes sociales son un facilitador global de contactos entre individuos y, cuanto mayor interacción, mayor es la huella que dejamos, **la información que se nos arrebató** y la posibilidad de perfilar nuestra identidad digital. [La dinámica impulsada por las compañías tecnológicas](#), y ahora por los Gobiernos e incluso por la Unión Europea, hace que nuestras interacciones sociales, políticas y culturales se produzcan a través de las redes sociales, incrementando nuestro tiempo de conexión.

El ‘yo’ digital ocupa un lugar preponderante en la normalización de las subjetividades

Además, nuestra identidad cambia con la aparición de nuevos espacios digitales. Hemos pasado de habitar Facebook a Twitter, aunque las nuevas generaciones viven en otros espacios como TikTok. Cada una de estas repúblicas digitales tiene sus propias reglas de etiqueta, mecanismos de extracción y aglomeración de la información. Eso sí, gracias al aprendizaje automático, el reconocimiento facial y otras técnicas, nuestro ‘yo’ digital, en sus bases de datos y conocimiento, **es más exacto y –quizá por eso– más peligroso**.

Este conocimiento casi íntimo produce una mutación en la forma en la que percibimos la realidad, con algoritmos que guían –ellos aseguran «facilitar»– nuestra navegación en el mundo digital, produciéndose así un cierto mecanismo de control social. El caso de [Cambridge Analytica](#) es un ejemplo fehaciente de la capacidad de las redes para identificar de forma precisa a un número importante de ciudadanos y

empujarles a cambiar su voto u opinión política. Nuestra identidad digital, usada como combustible para la inteligencia artificial, ocupa un lugar preponderante en el control, en el sometimiento y en la **normalización de las subjetividades**.

Podemos entrever es lo inevitable. La tecnología más fácil de usar, aquella que penetra en nuestro tejido social con más facilidad, aquella que, en definitiva, nos hace la vida más cómoda, acaba por imponerse. En este caso, se evidencia que no pasará mucho tiempo hasta que veamos cómo **la identificación facial se impone** en nuestros *smartphones*, ordenadores y, probablemente, como ocurre ya en China, en estaciones de tren, aeropuertos y espacios públicos. ¿Cuales serán las consecuencias?

Es tiempo de cuestionar los sistemas de relación entre humanos y máquinas, y el control de las máquinas sobre los humanos. Debido a las nuevas tecnologías, pasamos cada vez más parte de nuestra vida conectados a distintas redes y el 'yo' digital **amenaza con enseñarnos el rostro de nuestro Dorian Gray personal(izado)**.

Esteve Almirall es profesor de Operaciones, Innovación y Data Science en Esade. Ulises Cortés es catedrático de Inteligencia Artificial en la Universitat Politècnica de Catalunya.

[LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: Ethic

Fecha de creación

2021/08/22