Ciencia y TECNOLOGÍA

MUNDO DIGITAL

# Sousveillance: vigilar al vigilante

**Se sorprendería de cuánta información personal se divulga en una típica sesión matutina de internet**

J. Antonio García Macías*/ COLABORACIÓN
Ensenada, B. C. jagm@cicese.mx

En un pasaje del popular cuento infantil de Hansel y Gretel, los niños iban dejando un rastro de migajas de pan con el fin de poder ubicar el camino de regreso a casa. De manera similar, cada que nos aventuramos por los parajes del internet vamos dejando un rastro.

El problema es que por lo general no nos damos cuenta de ello, y de que hay empresas que están haciendo negocio con estos datos. ¿Se puede hacer algo al respecto?

## Tu información al mejor postor

El internet, las redes sociales, los dispositivos para comunicaciones móviles y otros elementos tecnológicos actuales han permitido estrechar lazos entre amigos, familiares, grupos profesionales y comunidades con intereses comunes.

Al usar estas tecnologías se comparte mucha información personal, en ocasiones de forma consciente, pero la mayor parte de las veces sin tener conciencia de ello. En efecto, el rastro digital que se va dejando incluye fechas de cumpleaños, lugares de residencia, preferencias políticas, creencias religiosas, lugares de trabajo, sitios donde se frecuenta ir a comer, relaciones personales, actividades profesionales y una larga lista que permite definir con mucha precisión el perfil de cada persona.

Algunos usuarios divulgan esta información conscientemente, o acceden a otorgar permisos que se les piden para hacerlo, con el propósito de recibir mejores recomendaciones sobre libros que leer, películas para ver en casa, personas con las que podría interesarle entablar alguna discusión y otros servicios "a la medida".

Sin embargo, el problema surge cuando no se les pide permiso a los usuarios para colectar su información y venderla a terceros, lo cual constituye una práctica usual y un negocio muy lucrativo. Tan lucrativo resulta que ese es básicamente el modelo de negocios que siguen empresas tales como Facebook, Google y muchas otras.

En un entorno fuera de internet, esto sería el equivalente a que alguien siguiera a las personas tomando fotografías, grabando películas y en general registrando las actividades que realizan para luego ir a vender la información. Por supuesto que esto resultaría inaceptable ¿pero por qué no protestan los usuarios cuando es una compañía de internet la que lleva a cabo estas prácticas?

## Vigilar a los vigilantes

En su libro "La sociedad transparente", aparecido en 1998, David Brin utiliza el término sousveillance acuñado por el investigador Steve Mann, para denominar el acto de que los subordinados, los vigilados, tienen ahora la capacidad de vigilar a sus vigilantes.

Dicho término es una palabra francesa donde el prefijo sous (debajo) da la idea de una vigilancia de abajo hacia arriba, en contraposición a surveillance donde el prefijo sur (sobre) indica la vigilancia en sentido contrario, o sea la supervisión.

Para darse cuenta de cuánta información se está divulgando al navegar por internet, así como de cuál información y quién la colecta, basta con instalar en el navegador algún agregado tal como "Ghostery" o "Collusion".

Quien lo instale seguramente se sorprenderá de cuánta información personal se divulga en una típica sesión matutina de ponerse al corriente con el correo electrónico y las redes sociales, así como revisar los noticieros online.

Aquí aplica la trillada frase de "conocimiento es poder", pues ahora se estará en posibilidad no solamente de conocer la información que se fuga, sino de actuar para decidir a quién autorizar y a quién prohibir que colecte información.

Durante el movimiento llamado "Primavera árabe" que inició en el 2010 se observó algo interesante: los mismos medios que sirven para vigilar a los ciudadanos pueden ser usados para vigilar a los gobiernos (o en general a quienes vigilan a los ciudadanos).

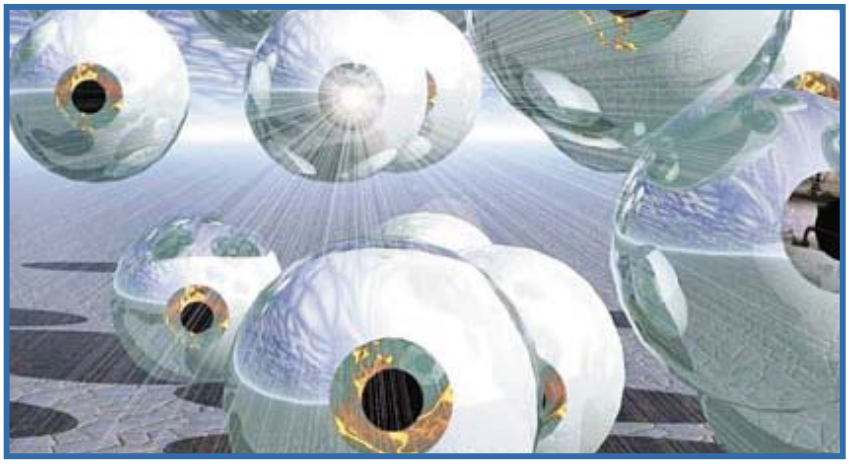
Fueron comunes las transmisiones de video en modo streaming, casi en tiempo real, que hicieron los ciudadanos dando cuenta de los abusos por parte de las autoridades. No importaba si después dichas autoridades llegaban a confiscar los teléfonos, cámaras u otros aparatos, pues la información ya había sido transmitida y todos habían podido ver lo que sucedía.

Pero el tener medios omnipresentes de reportes ciudadanos puede ser una arma de doble filo; cuando los agentes gubernamentales vieron las fotografías y videos enviados por los activistas, pudieron identificar a participantes y tomar represalias contra ellos.

Como consecuencia de esto, ya hay grupos que trabajan en el desarrollo de software que permita bloquear los rostros de participantes para no comprometer su seguridad. Ya no hay vuelta atrás, si son bien aplicadas estas nuevas tecnologías servirán de contrapeso a gobiernos opresores, permitirán a los usuarios controlar mejor su información y tener una seguridad más efectiva en el ciberespacio. Estamos siendo vigilados, es hora de vigilar a los vigilantes.

*El autor es investigador del Centro de Investigación Científica y de Educación Superior de Ensenada (Cicese).

Fotos: Cortesía



**Ahora se puede** *no solamente conocer la información que se fuga, sino actuar para decidir a quién autorizar y a quién prohibir que colecte información.*


**Las empresas** *de internet no piden permiso a los usuarios para colectar su información y venderla a terceros; una práctica usual y negocio muy lucrativo.*