

LA REGULACIÓN DE INTERNET DE LAS COSAS

La conexión de los ordenadores a internet fue la gran revolución tecnológica de las dos últimas décadas del Siglo XX. La conexión a internet de todos los demás aparatos y dispositivos, la llamada "internet de las cosas" (IoT) es sin duda la revolución tecnológica de las primeras décadas del Siglo XXI. Pero la vulnerabilidad de estos aparatos y dispositivos, que cada vez se incorporan a más actividades de nuestra vida cotidiana, desde el punto de vista de la privacidad, supone una amenaza creciente para la seguridad de los ciudadanos.

Diferentes instancias internacionales vienen advirtiéndolo de esas amenazas de *malware* que pueden afectarnos a través de cámaras de video, refrigeradores, televisores, enrutadores inalámbricos, altavoces y asistentes digitales, relojes, dispositivos de transmisión de audio / video, microordenadores, cámaras IP, DVR, equipos de antena, mando de puertas de hogar y de garaje o dispositivos de almacenamiento conectados a la red, entre otros. Con una simple llamada, los hackers pueden redirigir el tráfico a un sitio web donde capturan las contraseñas y los números de tarjeta de los consumidores (phishing).

Un reciente estudio del Cyber Security Research Institute norteamericano, denominado "Pinning Down the IoT" ponía de relieve que, en su forma actual, internet de las cosas representa una amenaza considerable para los consumidores debido a la falta de regulación, o a las regulaciones inadecuadas o ineficaces, sobre su seguridad de uso. También en EEUU, un estudio realizado en 2018 por el American Consumer Institute indicaba que 8 de cada diez enrutadores domésticos (a través de los cuales se conectan la mayoría de los otros dispositivos a internet) son vulnerables a los ataques de los ciberdelincuentes, incluyendo los de las principales marcas.

El problema tiene derivadas en ámbitos como la violencia de género: un reportaje de The New York Times en el que se entrevistaba a víctimas de esa violencia, puso de relieve que, en muchos casos, los acosadores utilizaban dispositivos inteligentes o manipulaban los de las víctimas para vigilarlas, controlarlas y mostrar su poder.

La consolidación de IoT requiere todavía de un desarrollo de la banda ancha que permita el lanzamiento eficiente de todos estos servicios (a través del 5G), pero entre tanto, los fabricantes, generalmente preocupados por crear dispositivos baratos y amigables en su uso, deberían también de aprender sobre las conexiones a internet seguras. Según señala F-Secure en un informe titulado "SmartHome. Old hacks, new devices", Google y Amazon han endurecido los estándares para sus dispositivos domésticos, invirtiendo miles de millones de dólares y con la colaboración de hackers éticos como Mark Barnes. Estas marcas hasta ahora se han mantenido en gran medida inmunes a los ataques a IoT, pero Google se vio obligado a anunciar a principios de 2018 que su sistema de seguridad Nest Security System incluía un micrófono del que no se había informado a los usuarios.

Las soluciones para afrontar estos riesgos pasan por la educación a los usuarios; por normativas y estándares claros y eficaces; por aplicar el criterio de la privacidad desde el diseño y la privacidad por defecto. En Europa, el Reglamento General de Protección de Datos debe ser una herramienta fundamental en este aspecto.

Ya en 2014 las Autoridades europeas de protección de datos aprobaron el primer Dictamen conjunto sobre internet de las cosas, valorando los beneficios económicos y sociales que puede suponer esta tecnología, pero también identificando y alertando de los riesgos que estos productos y servicios emergentes pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades.

El Dictamen planteaba el desarrollo de IoT en tres ámbitos: la denominada *wearable computing*, tecnología que se incorpora a la ropa o los complementos; los dispositivos capaces de registrar información relacionada con la actividad física de las personas, y la domótica. que, aunque en principio no recojan datos especialmente protegidos, pueden acabar proporcionando a terceros información inferida acerca de los individuos, configurando auténticos patrones de vida. Y las autoridades alertan, en este sentido, de que el usuario puede perder el control sobre la difusión de sus datos en función de si la recogida y el tratamiento de los mismos se realiza de manera transparente o no; es decir, se garantice su derecho al consentimiento informado sobre la finalidad de los datos recabados.