

Acuerdo entre la UE y EE.UU.: vía libre a la CIA para tener nuestros datos

El marco legal firmado este lunes 10 de julio sobre protección de datos deja más dudas que certezas para los ciudadanos europeos



Javier Villamor

Corresponsal en Bruselas 16/07/2023 Actualizada 17:00

La lucha entre la Unión Europea y Estados Unidos por la protección de datos ha terminado con un KO al viejo continente. Años de batallas judiciales entre usuarios y multinacionales del otro lado del Atlántico, con sonadas victorias para la libertad de los individuos, no volverá a repetirse. El acuerdo marco cerrado entre las dos potencias crea vías «legales y seguras» para que los servicios de inteligencia norteamericanos puedan acceder a información privada de los europeos por motivos de «seguridad».

Este acuerdo, nombrado ‘**Marco de Privacidad de Datos EU-EE.UU.**’, concluye que los niveles de protección aplicados en **Estados Unidos** son semejantes a los de la **Unión Europea**, cuando esto es radicalmente falso. En virtud de leyes como la *Foreign Intelligence Surveillance Act* (ley de vigilancia de inteligencia extranjera), las agencias de inteligencia estadounidenses pueden solicitar a las empresas acceso a datos sobre usuarios de otros países para garantizar la seguridad nacional.

No solo eso: poco después del **11-S** se aprobó –no tampoco sin polémica- la *Patriot Act* (ley patriota), mediante la cual el Gobierno podía espiar las conversaciones de todos los ciudadanos al ser alertado gracias a programas que reconocían determinadas palabras. Algo semejante se aplica en **España** con el programa **SITEL**, comprado en 2001 por el gobierno de **José María Aznar** pero puesto en marcha tras los atentados del **11-M**, ya bajo la presidencia de **José Luis Rodríguez Zapatero**. Como se puede apreciar, este tipo de medidas es la tónica general.

No hace muchos años hubo dos escándalos por temas semejantes. Uno, el de **Edward Snowden**, el famoso analista de inteligencia que filtró detalles de cómo funcionaban agencias como la **NSA** estadounidense. Otro, el espionaje de los Estados Unidos de **Barack Obama** a la Alemania de **Angela Merkel**.

¿Qué información se comparte?

Los países que se encuentran bajo la influencia estadounidense ya colaboran de manera activa al compartir este tipo de informaciones. En 1941 se creó la alianza de inteligencia ‘**Cinco ojos**’, formada por **Australia**, **Canadá**, **Nueva Zelanda**, **Reino Unido** y **Estados Unidos**. Estos países, todos de la esfera anglosajona, son parte del Acuerdo multilateral **UKUSA**.

La información compartida se divide en dos áreas. La primera se conoce como Inteligencia de comunicaciones (**COMINT**, por sus siglas en inglés). Hace referencia a las comunicaciones de voz interceptadas como llamadas telefónicas o correos de todo tipo. La segunda es Inteligencia electrónica (**ELINT**): uso de sensores electrónicos para señales de radares o sistemas de misiles tierra-aire.



Los ‘Cinco ojos’ tienen una versión ampliada, los ‘**Nueve ojos**’. A los cinco anteriores se les suman **Dinamarca, Francia, Países Bajos y Noruega**. Los nueve, a su vez, tienen otra versión ampliada, los ‘**14 ojos**’: al grupo anterior se unen **Bélgica, Alemania, Italia, España y Suecia**. Por otro lado, existe la obligación por ley a las empresas estadounidenses de dar todos los datos de sus usuarios a los servicios de inteligencia si no quieren ser multados. La privacidad brilla por su ausencia.

El que se opone a estas medidas es castigado legal o económicamente. **Yahoo** lo intentó en 2007 y en 2014 el Ejecutivo estadounidense amenazó con una multa diaria de 250.000 dólares a la empresa si no entregaba los datos de sus clientes a las agencias de inteligencia. El famoso motor de búsqueda fue a juicio para defender a sus usuarios y perdió. Y de esto hace ya un tiempo. Las cosas no han ido a mejor, tampoco para Europa.

Vías para la defensa

El marco de acuerdo introduce supuestas garantías como la creación de un tribunal para recursos específicos de violaciones de protección de datos. El ciudadano cuya privacidad considere que está siendo violada puede iniciar un proceso de reclamación que llevará su tiempo. Sea como sea, el tribunal se encuentra en suelo estadounidense, algo que dificulta la transparencia -cuando no anula- la supuesta imparcialidad del mismo.

Las empresas que deseen acceder a los datos europeos, deberán comprometerse a «borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida, y a garantizar la continuidad de la protección en caso de compartir los datos de carácter personal con terceros».

¿Un compromiso es suficiente? ¿Cómo se asegurará **Bruselas** de que se cumpla? Por otro lado, ¿cómo es posible que las leyes de protección de datos europeas, cuyas penas son millonarias para los infractores en nuestro suelo, no se apliquen a terceros interesados? ¿Es normal que una empresa estadounidense, que accede a los datos cedidos, pueda a su vez ceder estos a terceros en su país?

A estas preguntas intenta dar respuesta «órganos independientes e imparciales de impugnación». Por el momento, la primera revisión del marco de acuerdo se llevará a cabo antes de que se cumpla un año de la entrada en vigor.

Fuentes de ciberseguridad, al ser consultadas al respecto, lo tienen claro: «la mejor manera de proteger los datos es que no se muevan de donde están».