

Resolución

Rastreo en línea y privacidad



El rastreo en línea permite a los proveedores monitorear casi todos los aspectos del comportamiento del usuario en toda la red. El tipo de información que puede ser obtenida por medio del rastreo en línea (ej. dirección IP, aparatos de identificación, etc.) puede llevar a la identificación de un dato personal en particular. Esta posibilidad deja al descubierto un rico potencial para la creación de una minuciosa historia del uso completo del Internet de un sujeto identificable por períodos de tiempo potencialmente ilimitados.

Los datos sobre la actividad de los usuarios recopilados en una computadora u otro dispositivo (por ejemplo, un teléfono inteligente) durante el uso de los distintos servicios de la sociedad de la información en Internet son cada vez más coordinados, correlacionados y analizados para diversos fines que van desde la caridad para fines comerciales de los diferentes actores que ofrecen tales servicios o parte de los mismos. Los perfiles de intereses generados (o "perfiles de usuario") se pueden enriquecer con datos del "mundo real" en casi todos los aspectos de la vida privada, incluida la información financiera, así como información sobre, por ejemplo, el tiempo libre, la salud, las opiniones políticas y / o religiosas .

Reconocemos que este rastreo ofrece ciertos beneficios al consumidor, tales como manejo de redes, seguridad y prevención de fraude, y puede facilitar el desarrollo de nuevos productos y servicios. Sin embargo, este avance tiene un riesgo sin precedentes para la privacidad de todos los ciudadanos en una sociedad de información ya que podría conducir a anular y terminar con algunos de los principios básicos de la privacidad: transparencia, la limitación de los fines y el control de los individuos.

En consecuencia, los actores involucrados, específicamente los gobiernos, las organizaciones internacionales y los proveedores de servicios de la sociedad de la información tienen que asegurarse de que la protección de la privacidad en un futuro tenga más prioridad en el uso de los servicios de la sociedad de la información.

Por lo tanto, la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad convocan a los actores involucrados a:

- observar estrictamente el principio de la limitación de los fines;
- notificar y controlar el uso de elementos de rastreo, incluyendo aparatos de escaneo de huella digital;
- abstenerse del uso de elementos de rastreo invisibles en propósitos diferentes a los de seguridad/detección de fraude o manejo de redes;
- abstenerse de derivar un cúmulo de elementos de información (huella digital) con el único objetivo de identificar y rastrear usuarios en propósitos diferentes a los de seguridad/detección de fraude o manejo de redes;
- garantizar una adecuada transparencia sobre los diferentes tipos de prácticas de rastreo en línea para propiciar que los consumidores tomen decisiones de manera informada;

El Comisionado de Información de la República de Eslovenia y la Autoridad Francesa de Protección de Datos se abstuvieron de votar en esta Resolución.

- conceder amplio control a los usuarios sobre recolectar, retener, usar y compartir sus datos personales a través de mecanismos técnicos fáciles de utilizar;
- evitar rastrear a niños y en sitios dirigidos a ellos y en los que sea evidente la ausencia de supervisión paterna;
- respetar el principio 'privacidad por diseño' y llevar a cabo una evaluación de impacto sobre privacidad al inicio de nuevos proyectos;
- utilizar técnicas para reducir el impacto a la privacidad, tales como anonimato/ pseudo-anonimato;
- promover los estándares técnicos para un mejor control de usuario, por ejemplo, el estándar *Do-Not-Track*.