LAS COOKIES DE LA VIDA REAL

Internet ha cambiado

En los últimos años, los usuarios de Internet hemos asistido a un cambio drástico en la información adicional que ofrecen las páginas web europeas.

A finales de los 90, ejércitos de pop-ups publicitarios nos atacaban al entrar en cualquier página.

Web 1999

Mirando el lado bueno de las cosas, estos pop-ups ayudaron a muchos usuarios noveles a conocer y evitar algunos riesgos de Internet (dialers, spyware, adware…), y a mejorar su destreza en el cierre de ventanas no deseadas como si de un videojuego se tratase.

Superada esta fase, el motor de internet (la publicidad) maduró y se racionalizó.

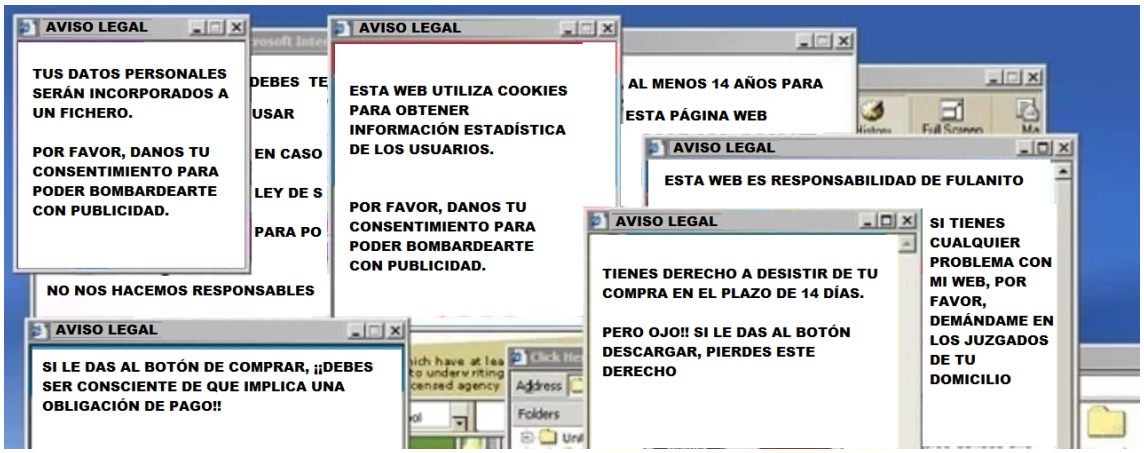
Los pop-ups se fueron abandonando poco a poco (salvo en algunas webs de dudosa reputación), los banners se limitaron de forma que no afectaran al contenido que buscaba el usuario, y la publicidad no gráfica de Google asumió el control global de este mercado.

Para hacer viable esta evolución, fue necesario desarrollar una tecnología que permitiese a las webs obtener cierta información del usuario sin necesidad de su intervención directa (las famosas cookies), mejorando la experiencia de uso y minimizando las molestias del usuario.

Con las cookies puede medirse la efectividad de los anuncios, el número de usuarios únicos, conocer los intereses de los usuarios y perfilar los anuncios según su perfil. Todo ello de forma sigilosa, y sin que el usuario medio fuese consciente.

Pero aprovecharse de la inconsciencia del usuario (aunque sólo sea para mantener un modelo de negocio sin molestar al usuario en demasía) no está bien visto. En Europa no.

Por ello, el Legislador Europeo ha dirigido un contraataque contra las cookies con una nueva legión de pop-ups, esta vez para informar sobre el uso de las cookies, que recuerdan mucho a aquella molesta fase inicial.



Web 2014

¿Se acabó la anestesia mental… la renuncia a tener un conocimiento efectivo de lo que hacen estas tecnologías con nuestros datos? Nada más lejos de la realidad. Aplicamos la destreza obtenida para cerrar pop-ups a golpe de clic y nos libramos del incordio de turno.

Ni una cosa ni la otra. Lo cierto es que el usuario no quiere barreras que se interpongan entre el contenido que quiere y él… ni publicitarias ni legales.

De hecho, algunos usuarios empiezan a considerar la necesidad de un bloqueador de avisos legales: un “Legal Advise Block” como evolución de los actuales bloqueadores de publicidad.

El salto al mundo real

Ahora, una nueva tecnología asoma en el horizonte: “Internet Of Things” (IOT) o el “Internet de las Cosas”. Una nueva oportunidad de negocio, que ofrece al usuario unos servicios futuristas y una vida más fácil, a cambio de mantener su inconsciencia voluntaria.

Gafas, relojes, teléfonos, cuantificación biométrica, electrodomésticos, papeleras… todo inteligente, o mejor dicho, todo conectado a internet y con capacidad para prestar servicios adicionales.

Las empresas están encantadas con esta nueva oportunidad, y los usuarios hacen colas kilométricas para obtener el último gadget.

¿Y cuál es el problema?

- Notificación: “*Ey, en la tienda por la que acabas de pasar tienen en oferta las zapatillas que estuviste mirando ayer por internet y que no compraste porque estaban demasiado caras.*”

- Notificación: "*Ey, llevas varios días sin moverte lo suficiente. ¿Quieres ofertas de los gimnasios de tu zona?*"
- Notificación: "*Ey, por las compras realizadas con el monedero virtual, parece que estás fumando tanto como el 75% de las personas que han sufrido un cáncer de pulmón en los últimos 10 años. Deberías consultar con tu médico. ¿Quieres saber cuál es el centro oncológico más cercano?*"
- Notificación: "*Ey, se te está acabando la leche desnatada sin lactosa, ¿quieres que pida más a tu tienda de alimentación online?*"
- Notificación: "*Ey, veo que has estado varias horas en un local de carretera, ¿quieres contratar un servicio de coartadas?*"

Nuevamente, las autoridades europeas detectan que estas tecnologías se aprovecharán de la consciencia anestesiada de los usuarios para obtener un rédito económico (aunque sea indirecto).

Es decir, estos nuevos gadgets no sólo cubren una necesidad tecnológica (llamar, hacer fotos, buscar información en Internet, etc.), sino que simulan una especie de mayordomo, asesor y entrenador personal que no es totalmente desinteresado y que se alimenta de la información que obtiene del usuario de forma sigilosa… Como las cookies, pero en el mundo real.

Reacción de las autoridades en materia de protección de datos

Es por ello, que el Grupo de Trabajo del Artículo 29 ha elaborado el Dictamen 8/2014 sobre la evolución del Internet de las Cosas, centrándose en los siguientes puntos:

1. Alcance del Dictamen:
   a. Wearable Computing: Referido a la ropa y accesorios con capacidad de conexión a internet, y uso de aplicaciones. Actualmente, los 2 mayores exponentes son las gafas y los relojes.
   b. Auto cuantificadores: Referido a medidores de parámetros biométricos: respiración, tensión arterial, ciclos de sueño, peso, etc. Aunque se exponen de forma separada, en realidad, es algo que ya incorporan la mayoría de los *smart wearables*.
   c. Domótica: Quizá es la más antigua de las tecnologías, pero hasta ahora no termina de despegar por su elevado precio. Básicamente se traduce en la informática aplicada al hogar (electrodomésticos "inteligentes", regado de plantas, seguridad de la casa, temperatura, ahorro de electricidad, etc.)

2. Riesgos detectados:
   a. Falta de control sobre la información personal que se obtiene de forma directa e indirecta: Abriendo la puerta a una posible sobreexposición no deseada por el usuario.
   b. Vicios en el consentimiento**:** Si el usuario no conoce todas las posibilidades del dispositivo, su consentimiento no será completo. Además, en muchos casos no se prevé un diseño de la privacidad, por lo que el usuario podría sentirse cautivo por el deseo de usar el dispositivo.

c. La inferencia o deducción de otros datos: Estas tecnologías permiten obtener datos que en bruto no tienen sentido, pero que comparándolos con otros, pueden dar más información de la que el usuario sabe de sí mismo**.**
d. Obtención de perfiles y patrones: Con toda esta información, un fabricante puede saber que el 85% de las personas que hacen X, compran Y, estableciendo patrones de conducta y perfiles sobre los usuarios que puedan ser explotados.
e. Dificultades o limitaciones para permanecer en el anonimato**:** Derivado de lo anterior, el GT29 detecta también posibles riesgos para el anonimato de los usuarios.
f. Seguridad de la información: Y como colofón a todos los riesgos anteriores, se expone cierto temor a que se priorice la facilidad de uso de los dispositivos por encima de la seguridad (no sólo de los dispositivos, sino también de la información que transmiten por redes de comunicaciones).

3. Aplicabilidad del derecho de la UE

   A pesar de lo discutible que resulta, el GT29 entiende nuevamente aplicable el criterio utilizado en el caso Google, por el cual se aplica la normativa europea cuando se utilizan "equipos" situados en el territorio de uno de los estados miembros.

   Recordemos que en el caso Google, se estimó aplicable la normativa europea, porque Google almacenaba datos de los usuarios en las cookies que, a su vez, se almacenan en los navegadores y equipos de los usuarios.

   Parece claro que Google recurrirá este criterio, que, potencialmente, le obligaría a cumplir con todas las legislaciones locales de los países en los que haya usuarios de sus servicios.

   En todo caso, en mi humilde opinión, es ponerle puertas al campo.

   No tardaremos en ver una nueva tecnología similar a las cookies, pero que no almacene información en el equipo del usuario, sino en una nube que quede bien lejos de la UE.

   Aplicando estas medidas a todos los dispositivos IOT, los fabricantes y desarrolladores ubicados fuera de la UE podrían esquivar la aplicación de una normativa tan "incómoda" para ellos.

   Por otra parte, el futuro Reglamento Europeo de Protección de Datos podría dar un paso más y obligar a todas las empresas, independientemente de su ubicación física, a cumplir con la normativa europea cuando se manejen datos de ciudadanos europeos.

4. Obligaciones de los responsables

   Mientras no se produzca este cambio en el almacenamiento de la información, los responsables de los datos obtenidos a través de estos dispositivos IOT tendrán que cumplir con todas las obligaciones de la normativa europea: informar, obtener consentimiento, garantizar la calidad y seguridad de los datos, así como reconocer los derechos de acceso, rectificación, cancelación y oposición por parte de los usuarios.

   Todo ello bajo la amenaza de cuantiosas sanciones económicas.

Opinión

La pelea entre las autoridades europeas y las empresas de la economía basada en Internet se va a endurecer aún más en los próximos años.

Y en medio de esta pelea, están los usuarios que únicamente quieren asomarse al futuro sin preocuparse por el precio (sea cual sea).

¿Deben las autoridades europeas mantener una lucha en nombre de los derechos de los usuarios cuando ellos no están preocupados?

¿Es totalmente desinteresada esta lucha por parte de las autoridades europea o hay cierto interés recaudatorio, escudándose en un derecho fundamental de sus ciudadanos?

El tiempo lo dirá.

José Carlos Moratilla

Responsable del Departamento Legal

Áudea Seguridad de la Información, S.L.