

GUÍA LEGAL: LA PUBLICIDAD MOBILE

1

¿DE QUÉ ESTAMOS HABLANDO?

No cabe ya ninguna duda de que dispositivos móviles, como los smartphones o tablets, forman parte inseparable de la vida de las personas. De hecho, tal y como recoge el [Estudio Mobile 2015](#) de IAB, se estima que en España, de los 18,2 millones de internautas de 18 a 55 años, un 89% posee un terminal móvil, y que mayoritariamente será un smartphone, lo que genera un dimensionamiento de 15,4 millones de individuos internautas. Estos datos, que crecen anualmente, han hecho que desde hace tiempo las empresas hayan puesto el foco de sus estrategias de comunicación digital en estos dispositivos.

De hecho, ya no se entiende un dispositivo móvil como un mero receptor de contenido, si no que además es una herramienta que permite aportar gran cantidad de datos e información de las personas. En esta guía abordaremos algunas de las cuestiones principales que se han de tener en cuenta a la hora de realizar acciones publicitarias a terminales móviles: desde la recogida y uso de datos personales, a la forma de presentación del contenido.

2

¿CÓMO SE REGULA EN ESPAÑA?

Como siempre, aportamos en unas líneas la normativa de referencia que se aplicará a las acciones de publicidad orientadas a terminales móviles. Será de aplicación toda la normativa habitual que afecta al sector, si bien, dependiendo de las acciones que se realicen y el modo de llevarlas a cabo, tendrán una mayor incidencia algunas de las siguientes normas:

- Ley 34/1988, de 11 de noviembre, General de Publicidad
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD).
- Ley 3/1991, de 10 de enero, de Competencia Desleal.

3

LA INFORMACIÓN OBTENIDA DEL TERMINAL COMO EJE FUNDAMENTAL

Una de las principales características de los terminales móviles es que pueden ser una gran fuente de información y de datos de su usuario, lo que permite que la publicidad sea mucho más específica e individualizada. Además, permiten también que sea el propio usuario el que reciba la publicidad de forma general, como puede ser al navegar por Internet desde su dispositivo, o de forma personalizada, por ejemplo a través de aplicaciones móviles, comunicaciones directas, o sistemas de conexión, como el bluetooth o el NFC.

De hecho, los dispositivos móviles ofrecen una relación bidireccional: por un lado el anunciante puede llegar con su mensaje al usuario allá dónde esté, y por otro, puede obtener datos de éste para crear y ofrecer una publicidad más dirigida.

Cuando hablamos de móviles, intrínsecamente relacionadas están las aplicaciones o 'apps', que son herramientas útiles con las que, a través de sus registros de usuarios y logins sociales, recoger datos, en muchas ocasiones para el envío de comunicaciones comerciales, y también para que sirvan como plataformas desde las que servir publicidad.

Pero además, los móviles, a través de su tecnología, también permiten captar y recibir publicidad empleando funcionalidades como la geolocalización, las conexiones bluetooth, wifi o NFC.

En lo que respecta a la obtención de datos del usuario por el uso de su teléfono o tablet, debemos partir del cumplimiento de los principios generales de la Ley de Protección de Datos, a los que hay que añadir también las reglas de las comunicaciones comerciales de la LSSI en caso de que los datos se empleen para esta finalidad. Básicamente, recordando lo que se ha comentado en otras guías se debe tener en cuenta:

- **Información:** La cuestión básica inicial es ofrecer al usuario, antes de la recogida de sus datos, información clara sobre el titular, el recabado de datos, su finalidad y la forma para ejercer sus derechos. Cuando además entran en juego sistemas técnicos específicos (más allá de registros y datos introducidos por el propio usuario), como pueden ser los datos de geolocalización, cookies, o sistemas de comunicación (Bluetooth, Wifi, RFID o NFC), se debe ofrecer además, información específica sobre su uso y las formas de desactivarlos, o en su defecto, de no ser posible, informar de dicha circunstancia de forma previa.

La geolocalización ha sido considerada por las autoridades europeas de protección de datos como especialmente invasiva de la privacidad del usuario y, por ello, se ha actuar con cautela con su uso, por lo que optar por la obtención de un consentimiento específico, la renovación periódica de este consentimiento (al menos, anualmente) o la advertencia continua al usuario, a través de su terminal, de que está siendo geolocalizado.

- › No sólo se debe ofrecer información sobre la recogida de datos, sino también de las implicaciones que pueden entrañar el uso de ciertas funcionalidades, por ejemplo, el consumo de datos que podría afectar a la factura del teléfono del usuario.
- › Además, también se debe informar de acciones concretas que el usuario puede hacer con distintos tipos de aplicaciones, como son las medidas para que comparta toda su agenda de contactos o sistemas del tipo 'member get meber' (MGM), que tienen unas obligaciones especiales.

- **Consentimiento.** Cuando los datos se recaben para ser empleados con fines publicitarios, además de esta información, será necesario contar con el consentimiento del interesado. En función del medio por el que se le vaya a enviar esa publicidad, ese consentimiento tendrá que ser expreso o, por el contrario podrá ser tácito.

- › Por ejemplo, cuando la publicidad vaya a ser realizada por correo electrónico u otro medio de comunicación electrónica equivalente (como mensajes, whatsapp u otros sistemas de mensajería instantánea como los mensajes generados por las apps), sí será necesario el consentimiento previo y expreso.
- › En cambio, si la publicidad no se generará por esos canales, y por ejemplo será servida en el contenido al que acceda el usuario (banners, videos, etc.), bastaría en principio con un consentimiento tácito.

- **Facultad de control:** Sin embargo, además de todo lo anterior, el usuario debe poder tener control sobre las funcionalidades de las aplicaciones y el envío de datos de éstas. Establecer sistemas técnicos que permitan al usuario desconectar ciertos servicios y/o recordarle cómo hacerlo a través de las opciones de configuración de su dispositivo es una cuestión muy relevante.

La clave está en que el usuario pueda desactivar de forma previa ese tipo de servicios para su uso publicitario, por ejemplo ofreciendo la posibilidad de desactivar la recepción de notificaciones de la aplicación, la geolocalización, etc.

Además de lo anterior, se ha de tener en cuenta la cantidad de datos que se pueden obtener de los terminales móviles y sus aplicaciones: los wearables, por ejemplo, generan información biométrica, relacionada con la salud, hábitos y movimientos, algo que unido al GPS u otros sistemas de localización, permiten obtener hasta una trazabilidad del usuario. En este sentido, el hecho de poder recabar esos datos no implica de entrada que se pueda hacer, y deberemos atender el principio de proporcionalidad y el de calidad de los datos.

- › Resulta primordial especificar qué datos se van a obtener, y esto se debe hacer siguiendo el principio de calidad de los datos: solicitando exclusivamente aquellos que son necesarios para las finalidades con que se pretenden usar. También realizar un juicio de proporcionalidad ayudará a no extralimitarnos en el uso de datos personales.
- › Muchas aplicaciones acceden a los datos de los contactos que el usuario tiene en su agenda. No está de más recordar al usuario que deberá ser él quien informe de ello a sus contactos y recabe su consentimiento.
- › También, no deben quedar en el olvido que se deben establecer medidas de seguridad adecuadas para impedir la interceptación de datos por terceros ajenos, algo que la Agencia Española de Protección de Datos ya ha tratado en varias ocasiones en relación al NFC y al bluetooth.

En lo que respecta a las cuestiones legales aplicables a la publicidad servida a los terminales móviles, lo cierto es que no hay mucha variación respecto a la normativa general, salvo por el dispositivo receptor.

En este caso, al igual que lo comentado en el apartado anterior, se deberá de analizar separadamente aquella publicidad que sea comunicada mediante comunicaciones electrónicas como el email, de aquellas que no lo sea.

En el primero de los grupos, destacan cuestiones relevantes en cuestiones tales como:

- **Información:** De forma general se debe ofrecer una información básica sobre la publicidad y el anunciante.

- › Las comunicaciones comerciales deben ser fácilmente identificable como tales. Hasta hace poco, la norma exigía que se establecieran palabras como PUBLICIDAD o PUBLI en los mensajes o contenidos, si bien con la última modificación legal, basta con que quede suficientemente claro que se trata de comunicaciones comerciales.

- › Además, en cualquier tipo de publicidad debe quedar claro quién es el anunciante, bien identificándole como tal, bien con una clara referencia a su marca.

4

SUMINISTRAR PUBLICIDAD: MISMAS REGLAS, DISTINTO ENFOQUE

• **Facultad de control:** Ligado a lo anterior, en cuestiones relacionadas con comunicaciones comerciales, destaca la obligación de ofrecer medios para que pueda oponerse a recibir ese tipo de publicidad también de forma posterior. Y en relación a la publicidad servida a través de las comunicaciones inalámbricas de los terminales móviles, esta facultad de control se debería de ampliar a permitir un control técnico sobre esas funcionalidades.

› En el primero de los casos, un sistema de notificación por email, o links que gestionen bajas automáticamente, serán medios muy útiles para cumplir estos fines.

› Para el segundo de los casos, en los que la publicidad puede aparecer en un terminal móvil por el simple hecho de pasar por delante de un escaparate, o acercar el móvil a un dispositivo emisor, también deberían implantarse medidas que permitan al usuario poder oponerse a esa recepción, especialmente si no ha sido informada o consentida previamente.

Por otra parte, en relación con acciones publicitarias destinadas a contenidos, como pueden ser banners o ventanas emergentes en aplicaciones móviles o en Internet, se debe tener en cuenta que el tamaño de la publicidad será relevante, especialmente para aquellas empresas que estén adheridas a un código de conducta, por ejemplo el de Confianza Online.

En este caso, las obligaciones pueden ir un poco más allá de las legales, que en este caso concreto establece que la publicidad no debe impedir el uso normal de los terminales.

› A raíz de esta cuestión, una buena práctica será la de no impedir al usuario continuar navegando o utilizando sus aplicaciones con contenidos que ocupen toda o gran parte de la ya de por sí, reducida pantalla.

› También lo será, el hecho de que la publicidad pueda ser evitada por el usuario, algo que se consigue permitiéndole cerrar, salir o saltarse la publicidad para poder continuar con el uso normal del terminal.

El principal organismo competente para hacer cumplir las obligaciones en relación a la recogida, y tratamiento de los datos personales de los usuarios y la correcta atención de los derechos de éstos es la Agencia Española de Protección de Datos, cuyas multas, en los casos más graves, pueden llegar a alcanzar hasta 600.000 euros.

La Agencia Española de Protección de Datos también se ocupa de controlar el cumplimiento de las obligaciones en materia de comunicaciones comerciales por vía electrónica.

En cuanto a otras cuestiones relacionados con la publicidad o la competencia derivada de actos de publicidad ilícita, su control correspondería a los juzgados y tribunales, previa demanda.

5

¿QUÉ ORGANISMOS SON COMPETENTES PARA HACER CUMPLIR LA LEY?

iab
spain legal