8 de febrero de 2013

Posición de IAB Spain sobre la Propuesta de Reglamento europeo de protección de datos

IAB Spain es la asociación que representa al sector de la publicidad en medios digitales en España. Engloba a los diferentes actores del panorama publicitario online: agencias de medios, agencias creativas, anunciantes, soportes, redes, empresas de mobile marketing, de vídeo, de e-mail marketing, digital signage, buscadores, consultoras, observadores, medios de comunicación y proveedores tecnológicos.

El fin de IAB Spain, que en la actualidad cuenta con 180 empresas asociadas, se centra en impulsar el desarrollo de la publicidad, el marketing y la comunicación digital en España.

IAB Spain acoge favorablemente la armonización de la legislación en materia de protección de datos en la UE (y el Espacio Económico Europeo). Este avance debería facilitar a las empresas su expansión a otros mercados europeos, así como a los usuarios el uso de los servicios y la adquisición de bienes de otros países europeos con total confianza en su nivel de protección. Los problemas que planteó y plantea la aplicación de la Directiva de e-privacidad, cuando algunos países se han sobrepasado sus límites, no deben replicarse, y el Reglamento proporciona una oportunidad para rectificar este tipo de distorsiones:

- **La definición de datos personales: buscar una definición válida y uso de conceptos como datos anónimos y datos seudónimos (Art. 4 y 10)**

La Propuesta de Reglamento de la Comisión amplía la definición de datos personales para incluir «identificadores únicos», que incluyen chipsets, direcciones IP, cookies, o datos de ubicación. IAB Spain considera que la redacción actual es demasiado amplia y propone mantener el sólido marco de protección de datos que existe actualmente y aclarar el uso de **los datos anónimos y los seudónimos.** Este planteamiento **protegería mejor a los interesados** al mismo tiempo que permitiría a las empresas tratar los datos de manera legítima y más útil. Los datos anónimos deben excluirse explícitamente del ámbito del Reglamento mientras que los seudónimos requieren como salvaguardia adicional el derecho de oposición. En este sentido, sería necesario un régimen que incentive al sector privado a utilizar este tipo de información, en lugar de información identificable. El uso de datos seudónimos también facilita el análisis efectivo de datos en la investigación científica

Para más información puedes contactar con IAB Spain www.iabspain.net
Paula Ortiz, paula@iabspain.net Teléfono: 91.402.76.99

(incluyendo analítica). El enfoque de los datos seudónimos se establece en el Art. 15 (3) de la Ley alemana sobre Telemedios, y protege a los sujetos mientras que permite a las empresas realizar el tratamiento de algunos datos sin identificarlos.

- **La definición del consentimiento como explícito: mantener el régimen actual para evitar el incremento en las recogida de datos y establecer una relación con la Directiva de e-privacidad (Arts. 4, 7 y 8)**

La Propuesta de Reglamento exige que los responsables del tratamiento obtengan el consentimiento *explícito* cuando opten por este importante fundamento jurídico para el tratamiento de los datos personales. Aunque no hay duda de que el consentimiento explícito se justifica en numerosas situaciones, y especialmente cuando se realiza el tratamiento de datos sensibles, la extensión a casi todos los tratamientos de datos genera un efecto negativo: los consumidores se verían sin duda sobrecargados con solicitudes de consentimiento y podrían fatigarse por la cantidad de clics que deberán hacer. **Esta extensión junto con el cambio de paradigma para exigir la obtención del consentimiento explícito para muchas categorías de datos sitúa en una posición de desventaja al sector europeo.** Además, en el entorno internet, los diferentes agentes implicados ya realizaron los cambios, inversiones y desarrollos necesarios para cumplir con el actual régimen normativo, y resulta innecesario obligarles a revisar todas sus implementaciones a la luz de una nueva definición de consentimiento que el legislador no vio la necesidad de modificar en 2009. Además, el sector de internet europeo cuenta con un amplio segmento de empresas B2B. Si ya puede es difícil la obtención de consentimiento explícito para las empresas B2C, que mantienen actualmente una relación con los consumidores, el caso empeora para las empresas B2B. Si es una empresa B2B la que pide que otorguen su consentimiento explícito para, por ejemplo, colocar cookies, es muy improbable que lo acepten, ya que apenas conocen las empresas B2B y no utilizan ninguno de sus servicios. La imposición de un consentimiento explícito puede llevar a la imposición de cargas excesivas al sector de internet, sin que ello se traduzca necesariamente en una protección más eficaz. Por todo lo anterior, la fórmula consentimiento informado sería la que más se ajustaría al entorno de internet, siendo lo principal que el usuario o interesado esté correctamente informado, conociendo la trascendencia de sus decisiones. Además es importante utilizar únicamente el consentimiento cuando sea realmente necesario, permitiendo así el tratamiento de los datos anónimos y los seudónimos. Contar con una definición clara de los datos anónimos y los seudónimos, así como un régimen aplicable a este tipo de datos, es una condición indispensable para evitar las incertidumbres jurídicas.

- **Informes de datos agregados / Analíticas web (Art. 4, 83)**

Las empresas, las instituciones académicas y los gobiernos emplean datos agregados con numerosos fines, incluidas las investigaciones científicas y de mercado. Por ejemplo, los

partidos políticos desean saber qué porcentaje de los internautas totales accede a los sitios web de sus campañas. Los conjuntos de datos individuales se combinan y se categorizan en grandes grupos o categorías y estas categorías se unen para crear «informes de datos agregados». Muchas organizaciones públicas y privadas confían en estas técnicas, y el Grupo de Trabajo del Artículo 29 ha concluido recientemente[1] que la analítica web plantean muy pocos o ningún riesgo para la privacidad y deben estar exentas de la obtención del consentimiento conforme a la Directiva de e-privacidad. Estos datos sirven para desarrollar nuevos productos y servicios y continuar innovando. Este uso de los datos debe, por tanto, excluirse del ámbito del Reglamento en lugar de esperar a que se revise la Directiva de e-privacidad (tal como ha sugerido el Grupo de Trabajo del Artículo 29).

- **Marketing directo y elaboración de perfiles (Art. 19 y 20)**

El Reglamento debería permitir los casos en los que se analizan datos anónimos y seudónimos para, por ejemplo, anunciar un producto o predecir la compra de un producto. La segmentación permite a las empresas adoptar decisiones en función de unas variables, les faculta para seguir innovando y desarrollar nuevos productos y servicios. Por ello, se considera necesario establecer una definición más clara y de lo que se entiende por segmentación. Al usuario, no obstante, debería otorgársele el derecho a oponerse a dicho tratamiento, creándose así un enfoque equilibrado respecto del derecho a la privacidad y los intereses empresariales.

- **Tratamiento lícito (Art. 6)**

En el Artículo 6 se enumeran las condiciones en las que se puede realizar el tratamiento de los datos personales. Este no contiene los datos seudónimos, ya que esta categoría no se ha introducido en el Reglamento pese a su importancia práctica, su extendido uso y la codificación jurídica en Alemania (Art. 15(3) de la Ley sobre Telemedios). Numerosos sitios web utilizan seudónimos, un concepto que incrementa la protección de los datos al eliminar la posibilidad de identificar de forma directa a un sujeto. Permitir este tipo de tratamiento de datos seudónimos estaría amparado en el interés legítimo del responsable del tratamiento e incrementará la protección.

- **Tratamiento de los datos personales relativos a los niños (Art. 8)**

[1] Dictamen del Grupo de Trabajo del Artículo 29 del 04/2012 sobre la exención a la obtención del consentimiento para el uso de cookies: "*…No es probable que las cookies analíticas de primera parte generen un riesgo para la privacidad… …el legislador europeo podría añadir de la forma adecuada un tercer criterio con respecto a la exención a la obtención del consentimiento para el uso de cookies que se limitan estrictamente a fines estadísticos agregados y anonimizados de primera parte*".

Resulta confusa la inclusión de dos definiciones de edad diferentes en un mismo instrumento regulatorio, especialmente cuando no se definen ni explican claramente los requisitos y circunstancias que se aplican a cada grupo de edad. La actual propuesta de reglamento define "niño" como toda persona menor de 18 años en su Art. 4(18). Sin embargo, la única mención a los requisitos aplicables a un grupo de edad específico se encuentra en el artículo 8, que se refiere sólo a requisitos relacionadas con "los niños menores de 13 años" y a la "oferta directa de servicios de la sociedad de la información a los niños". Esta "definición por omisión" nos lleva a la conclusión de que cualquier servicio que no se considere parte de la "sociedad de la información" estará sujeto a diferentes requisitos para el tratamiento de datos del niño (menor de 18 años). Sin embargo, estos otros servicios y/o sus requisitos no se contemplan en ningún otro punto de este artículo ni de la propuesta de reglamento. La distinción entre el tratamiento de datos online y offline dentro de la definición de niño dibuja una línea innecesaria, confusa y potencialmente peligrosa, agravada por la definición por omisión utilizada actualmente para trazar esta distinción.

En este sentido, es fundamental para la aplicación efectiva del nuevo reglamento que el Art. 8, referente al "Tratamiento de los datos personales relativos a los niños" se modifique para establecer **una restricción única y clara independientemente del ámbito en el que este tratamiento tenga lugar**, mediante la eliminación de la especificación "en relación con la oferta directa de servicios de la sociedad de la información a los niños".

En segundo lugar, en relación con las **condiciones deben cumplir los padres o tutores para dar su consentimiento. El artículo 8 debería aportar más claridad respecto a lo que se entiende por "esfuerzos razonables"** por parte del responsable para obtener el consentimiento verificable.

- **Privacidad por defecto (Art. 23)**

Los conceptos serían aplicables a todos los tratamientos de datos aunque es importante reconocer que no puede existir una solución universal. Los distintos servicios requieren soluciones distintas. Una red social cuya función para compartir contenidos se encuentre deshabilitada protege la privacidad, pero no es de utilidad para el usuario. La tecnología evoluciona a un ritmo acelerado, y exigir la conformidad con un standard obligaría a las empresas a utilizar una norma específica que podría ser menos innovadora y protectora que las nuevas normas.

- **Derecho al olvido (Art. 17)**

Resulta técnicamente imposible imponer la supresión cuando el control sobre esa información no está garantizado (p. ej. cuando usuarios comparten y almacenan fotografías de otros usuarios). En cambio, el derecho de los usuarios a solicitar el bloqueo, tal como se establece en la Directiva actual en su Art. 12 (b) debería mantenerse, lo que sería mucho más pragmático. El derecho al olvido es una prolongación de derechos ya

existentes compatibles con el entorno digital, siendo necesario aclarar la responsabilidad que tiene cada uno de los sujetos que opera en la red, atendiendo a lo que la normativa establece y recoger las limitaciones que ésta en relación tienen los intermediarios.

- **Evaluaciones de impacto sobre la protección de los datos (Art. 33)**

Las evaluaciones de impacto sobre la protección de los datos representan una carga pesada y costosa para los responsables y los encargados del tratamiento que probablemente no tengan como resultado un incremento de la protección de los datos o la privacidad de los sujetos. Las evaluaciones de impacto sobre la privacidad no deberían confundirse con los requisitos de información para los interesados, elemento que se aborda en la Sección 2: Información y acceso a los datos. En el caso de que se realicen evaluaciones de impacto sobre la protección de los datos, deberá añadirse un nuevo apartado en el que se aclare que están protegidos por secreto profesional.

- **Notificaciones de las violaciones de datos (Art. 31 y 32)**

Aunque es importante notificar a los usuarios las violaciones de datos que generan problemas, en otros casos la notificación en las que no va a haber consecuencias negativas para los usuarios sólo les sobrecargarán. En lugar de aumentar la seguridad, es probable que provoquen un agotamiento por el exceso de notificaciones. Es esencial limitar las notificaciones a aquellos casos en los que existe una probabilidad razonable de que la violación ocasione un daño grave a los sujetos afectados.

- **Extraterritorialidad y la dimensión internacional (Art. 3)**

No es realista pretender abarcar todos los servicios en línea del mundo. Por ejemplo, un servicio argentino podría estar dirigido a usuarios argentinos y un argentino de España podría querer suscribirse al mismo. Resulta desproporcionado extender el ámbito de aplicación de la legislación sobre protección de datos a este tipo de casos. En su lugar, la extensión debería limitarse a los casos en los que una empresa ofrece «de forma específica e intencionada» servicios en el territorio de la UE.