RESPUESTA DE IAB SPAIN A LA CONSULTA PÚBLICA SOBRE LA ADAPTACIÓN AL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

Desde IAB Spain, agradecemos la oportunidad de participar en la consulta sobre la adaptación del Reglamento General de Protección de Datos y compartir la visión de la norma y quedamos a su disposición para aclarar o profundizar los puntos aquí reseñados.

Siguiendo la línea de la consulta pública, nos gustaría compartir con ustedes las preocupaciones que comparten las empresas aquí representadas, en aras de evitar contradicciones con la normativa internas y de introducir mejoras en relación con los aspectos del ordenamiento jurídico español que pueden ayudar a las empresas que operan tanto en España como en otros países europeos, a implementar el Reglamento General de Protección de Datos (en adelante RGPD).

1. Licitud del tratamiento de datos personales: consentimiento e interés legítimo.

El artículo 6 del RGPD fija las condiciones para el tratamiento lícito de los datos, entre los que se encuentran el consentimiento y el interés legítimo perseguido por el responsable del tratamiento o por un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado y/o tercero.

Tal y como recoge el art. 6 (2) el interés legítimo puede ser interpretado por los distintos Estados Miembros fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo. En ese sentido, como ha reconocido el Grupo de Autoridades europeas de Protección de Datos en *su Dictamen 06/2014 sobre el concepto del interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* el interés legítimo ha de ser la legitimación fundamental para el tratamiento de datos personales, dado que es este fundamento es la única forma de legitimar el tratamiento cuando no es posible obtener el consentimiento del usuario.

Por tanto, el interés legítimo debería configurarse como la base jurídica fundamental para el tratamiento de datos en la futura ley de protección de datos en España.

No obstante, el art. 6 (4) introduce condiciones para el tratamiento posterior de datos personales que no responda a los fines iniciales de recogida, incluido el caso en que este tratamiento se fundamente en el interés legítimo. En ese sentido, recoge una serie de factores a abordar para establecer si el tratamiento de datos para un nuevo fin es compatible con los fines para los cuales se hayan recogido inicialmente los datos, como el contexto, la relación entre los fines originales y los posteriores y las posibles consecuencias para los interesados, entre otros.

Al respecto consideramos, siguiendo el dictamen del Grupo de Trabajo del Artículo 29, que una lista exhaustiva de intereses legítimos articulada en una ley puede ser demasiado rígida y no poder responder al entorno en constante evolución como el que nos encontramos. Por tanto, sería necesario abordar una normativa basada en principios que recojan que este interés legítimo ha de poder utilizarse tras un análisis equilibrado para facilitar el tratamiento de los datos al tiempo que protege los derechos de los interesados.

De esa forma solicitamos al legislador español a mantener el espíritu del RGPD en su literalidad, de modo que se pueda dar una aplicación flexible de estos criterios. Así se afianzaría un texto a prueba de futuro, permitiendo la innovación, lo que supone una gran ventaja para el conjunto de la unión y para los usuarios.

Entre los ejemplos que podrían darse en los que el interés legítimo puede jugar un papel importante podríamos reseñar el tratamiento de datos para el desarrollo de tecnologías innovadoras como *Big Data*, *Internet of Things*, *Machine Learning* e inteligencia artificial o la utilización de datos por parte de prestadores de servicios de intermediación en la sociedad de la información, dado que en multitud de situaciones el hecho de que a priori no haya relación entre el fin inicial de la recogida y el nuevo fin secundario, no convierte este fin en incompatible.

Otra de las legitimaciones que recoge el RGPD es el consentimiento, que todavía necesitará ciertas aclaraciones sobre su aplicación, dado que el texto se refiere a un consentimiento expreso y uno inequívoco sin

determinar los límites de ambos.

Al respecto es importante la mención a un aspecto de vital importancia: Cómo se han de tratar los datos que han sido recogidos hasta el momento usando como legitimación el consentimiento teniendo en cuenta la actual normativa. La futura ley debería contener mecanismos operativos por los que, con las garantías adecuadas, autorice a los responsables a seguir usando esos datos que se recogieron con el consentimiento, y sobre todo aquellos que se recabaron con el consentimiento tácito, lo que supone conforme a la normativa en el ordenamiento actual. De otra forma, toda una industria estaría incumpliendo, habiendo implantado las medidas de cumplimiento necesarias en el momento de la recogida y posterior tratamiento.

2. Finalidades

Respecto a las finalidades, el RGPD establece que estas habrán de ser específicas. Esta redacción debe interpretarse de manera que los diferentes modelos de negocio del entorno digital no sean puestos en riesgo de incumplimiento. Y es que la mayoría de los servicios y contenidos digitales se financian con la publicidad. De esa forma, la prestación de determinados servicios está sujeta a la aceptación de la recepción de publicidad. Si el servicio se ofrece de manera gratuita, debería poder condicionarse a la aceptación del tratamiento de esos datos para ofrecerle publicidad, que es la forma de financiación de ese servicio. En ese sentido también lo recoge la Propuesta de Directiva sobre contenidos digitales.

3. Menores

Al respecto del consentimiento, el RGPD introduce novedades, y limitaciones a la capacidad de consentir de los menores de 16 años, dejando no obstante a los Estados miembros la posibilidad de establecer una edad menor, nunca por debajo de 13 años.

En España, nuestro ordenamiento reconoce la capacidad del menor de prestar un consentimiento válido, en diversos artículos del Código Civil o en la Ley de Protección Jurídica del Menor en varias cuestiones que admiten

que el menor puede dar el consentimiento cuando tenga suficiente madurez, y en todo caso, cuando tenga más de 12 años.

En esa línea, los Tribunales también han reconocido que los menores pueden y deben prestar su propio consentimiento en casos que afecten directamente a sus derechos.

Por tanto, los límites a la capacidad de obrar del menor deben ser interpretados de un modo restrictivo, tal y como establece la Exposición de Motivos de la Ley de Protección Jurídica del Menor.

Diferentes normativas internacionales fijan la edad de 13 años como aquella en la que se alcanza la madurez, y se pueden llevar a cabo diferentes actos jurídicos.

Las tecnologías de la información constituyen una parte esencial de la educación de los menores en la actualidad y el acceso a las mismas es fundamental para asegurar un adecuado nivel educativo. Por tanto, no se pueden poner trabas innecesarias al acceso autónomo e independiente por parte del menor a estas tecnologías, garantizando una protección al menor a la vez que se le dota de herramientas y no se restringen sus libertades y derechos.

4. Elaboración de perfiles y decisiones automatizadas

Los interesados tendrán derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sería necesario aclarar qué son los efectos jurídicos o similares que afectan significativamente al afectado (los considerandos se refieren por ejemplo a la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna), pero faltaría una definición de lo que se considera efectos legales o que afecten de forma similar. En ese sentido, por ejemplo, mostrar una publicidad u otra en función de un análisis no produce efectos jurídicos en los términos definidos por el Reglamento.

5. Portabilidad de datos

El Art. 20 establece que el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado. Al respecto, el RGPD resulta ambiguo en algunos puntos que sería necesario aclarar en aras de una mayor seguridad jurídica, en la línea en la que lo ha hecho el Grupo de Trabajo 29 en su borrador de directrices sobre portabilidad en el que se aclara, por ejemplo, el formato, la necesidad de autenticación y las fuertes protecciones para el proceso de portabilidad. Y de suma importancia es el hecho de aclarar que los datos inferidos no sean objeto de este derecho, si no solo a aquellos que se han aportado activamente por el usuario.

Por otra parte, sería útil tener un mayor reconocimiento por parte de las Autoridades de Protección de Datos del derecho del responsable del tratamiento a proteger su propiedad intelectual, dado que al tener que proporcionar los datos en un formato interoperable (y no simplemente proporcionar acceso), las empresas pueden tener que compartir con sus competidores su método de recopilar, estructurar y utilizar estos datos y velando por el secreto industrial

6. Derecho de Supresión

El RGPD recoge el derecho al olvido estableciendo que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan.

El artículo está muy alienado con la TJUE en su sentencia de 13 de mayo de 2014, en el caso C-131/12. No obstante, es necesario que la ley aclare algunos aspectos, como el ámbito territorial cómo debe implementarse en la Unión Europea, y su interrelación con jurisdicciones de países extracomunitarios que no reconocen, no regulan, o lo hacen de manera diferente, este derecho.

Una solución a tener en cuenta puede ser el uso de la geolocalización para restringir el acceso a las URLs bloqueadas en todos sus dominios, que cumple con los criterios del TJUE.

7. Ventanilla única y mecanismos de colaboración

Respecto al mecanismo de ventanilla única, el establecimiento principal de los responsables y/o encargados del tratamiento es clave para determinar la competencia de la Autoridad de Protección de Datos principal.

En este sentido, este mecanismo tendría que ser reconocido en la legislación española para asegurar un funcionamiento efectivo. Por otro lado, sería importante que la Unión Europea trabajara en unas directrices que reafirmen la interpretación de lo que se recoge en la legislación española dado que es fundamental que e funcionamiento de este mecanismo sea en coordinación de todas las autoridades de protección de datos europeas.