La protección de datos personales debe ser un derecho fundamental

El consentimiento explícito para el tratamiento se ha convertido en una pieza fundamental del sistema legislativo

Se abre la puerta a la creación de planes de prevención, que si son eficaces, podrán servir para reducir la responsabilidad

En este ámbito, como ya va siendo habitual en todos los aspectos societarios, se impone la tendencia preventiva que ya impera en los ámbitos del blanqueo de capitales, de los delitos en el seno de la empresa o de los accidentes laborales. Esta tendencia abre la puerta a la creación de planes de prevención, que si se puede demostrar que son eficaces, podrán servir para reducir la responsabilidad. Valorar esta prevención cada vez es más necesario, puesto que se trata de datos personales dentro de los que se engloban cualquier información que permita identificar o hacer identificable a su titular, algo que las nuevas tecnologías y la investigación ponen cada vez más difícil.

El Reglamento General de Protección de Datos, que llega desde la Unión Europea, ha venido cargado de novedades y con un plazo máximo de dos años para que empresas y entidades, incluidas las públicas se adapten a las nuevas exigencias.

En este ámbito, como ya va siendo habitual en todos los aspectos societarios, se impone la tendencia preventiva que ya impera en los ámbitos del blanqueo de capitales, de los delitos en el seno de la empresa o de los accidentes laborales. Esta tendencia abre la puerta a la creación de planes de prevención, que si se puede demostrar que son eficaces, podrán servir para reducir la responsabilidad de las empresas.

Valorar esta prevención cada vez es más necesario, puesto que hablamos de datos de carácter personal dentro de los que se engloban cualquier información que permita identificar o hacer identificable a su titular, algo que con el avance de las nuevas tecnologías y la investigación cada vez es más difícil. Se trata de un derecho fundamental que reconoce al ciudadano su facultad de controlar los datos personales y le dota de la capacidad para disponer y decidir sobre los mismos.

Aunque lo más molesto pueda ser el empleo que el marketing y la publicidad pueden hacer de los datos personales, detrás de su tratamiento se esconden muchos peligros, ya que de no regularse y supervisarse, su uso el campo de las discriminaciones de derechos fundamentales puede estar en juego. Las posibilidades que permiten en la actualidad los análisis sobre el ADN o el genoma, así como otros marcadores biológicos, hacen que en manos descontroladas puedan convertirse en un grave peligro. Se trata, además, de impedir las discriminaciones por razones de edad, sexo, religión o raza, que no tengan fundamentos moral y legalmente accesibles.

Por ello, el consentimiento explícito para su tratamiento se ha convertido en una pieza fundamental del sistema legislativo de la protección de datos. El nuevo Reglamento acaba con el consentimiento tácito, con el consentimiento por silencio del titular de los datos, una auténtica rareza dentro del sistema legislativo comunitario. A partir de ahora, las empresas deberán ponerse al día y recabar estos consentimientos si no quieren ser duramente sancionados.

ISTOCK

La Agencia Española de Protección de Datos y, en su medida, las correspondientes a las comunidades autónomas, tienen una ardua tarea de información, mentalización, formación y control sobre todo, este gran procedimiento, que tiene una fecha de caducidad marcada: mayo de 2018.

Es loable el esfuerzo para dotar a las pequeñas y medianas empresas (pymes) de herramientas que faciliten la adaptación a la nueva normativa, que está llevando a cabo la Agencia y, máxime, si se tiene en cuenta que mantiene los mismos efectivos personales desde hace muchos años. La dirección de Mar España ha multiplicado las relaciones y los proyectos sin que el ánimo decaiga. Un gran mérito.

La Agencia Española de Protección de Datos y, en su medida, las correspondientes a las comunidades autónomas, tienen una ardua tarea de información, mentalización, formación y control sobre todo este gran procedimiento, que tiene una fecha de caducidad marcada: mayo de 2018. Es loable el esfuerzo para dotar a las pequeñas y medianas empresas (pymes) de herramientas que faciliten la adaptación a la nueva normativa, que está llevando a cabo la Agencia y, máxime, si se tiene en cuenta que mantienen los mismos efectivos personales desde hace muchos años. La dirección de Mar España ha multiplicado las relaciones y los proyectos sin que el ánimo decaiga. Un gran mérito.

Edita: Editorial Ecoprensa S.A. **Presidente de Ecoprensa:** Alfonso de Salas **Director Gerente:** Julio Gutiérrez
Relaciones Institucionales: Pilar Rodríguez **Subdirector de RRII:** Juan Carlos Serrano **Jefe de Publicidad:** Sergio de María

Editor: Gregorio Peña **Director de elEconomista:** Amador G. Ayora
Director de 'Iuris&Lex': Xavier Gil Pecharromán **Diseño:** Pedro Vicente y Alba Cárdenas
Infografía: Nerea Bilbao **Fotografía:** Pepo García **Redacción:** Pedro del Rosal e Ignacio Faes.

Nuevo Reglamento General comunitario

Llega la gran reforma en protección de datos

La Comisión General de Codificación valorará en los próximos meses los cambios normativos precisos para cumplir las exigencias comunitarias

XAVIER GIL PECHARROMÁN

El ministro de Justicia en funciones, Rafael Catalá -en la foto-, mostraba esta pasada semana en la 8ª Sesión Anual Abierta de la Agencia de protección de Datos (AEPD), su confianza en que la Comisión Europea pueda adoptar a corto plazo una decisión que permita "dotar de mayor fluidez a las transferencias de datos a EEUU con suficientes garantías para los derechos de los ciudadanos europeos".

Para Catalá, el hecho de que los mecanismos de transferencia internacional de datos no contemplen un nivel equiparable de protección podría producir un efecto indeseado para las empresas europeas "que se situarían en una situación de desventaja competitiva" frente a las de terceros países. Por ello, mantener la continuidad en la garantía del derecho a la protección de datos no sólo es "una exigencia" sino también "un elemento necesario para garantizar la competitividad".

Por ello, calificaba al nuevo Reglamento de Protección de Datos de la Unión Europea como "el principal hito en esta materia en los últimos años". Ante la aplicación de la nueva normativa, Catalá ha instado a todos los agentes implicados en el proceso a "aprovechar al máximo" este periodo transitorio para preparar la plena aplicabilidad del Reglamento.

En este contexto, el ministro ha señalado que "tenemos dos años de trabajo intenso por delante" y que "el reto de asumir el Reglamento no debe hacer olvidar las nuevas oportunidades de mejora que ofrece en la protección de los derechos de los ciudadanos". El Reglamento ha entrado en vigor el 25 de mayo de 2016, pero no comenzará a aplicarse hasta dos años después, el 25 de mayo de 2018. Hasta entonces, tanto la Directiva 95/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

En estos dos años a los que se refería el ministro en funciones, los Estados miembros deben adoptar o iniciar la elaboración de las normas necesarias para permitir o facilitar la aplicación del Reglamento. Esas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita.


F. VILLAR

Reforma de la legislación española

A este respecto, en otro foro - en la IV Conferencia Internacional de la Cátedra Google del CEU San Pablo-, la subsecretaria de Justicia, Aurea Roldán, anunciaba que la Comisión de Codificación del Ministerio de Justicia iniciará los trabajos de análisis y reflexión sobre la necesidad o no de elaborar una nueva Ley Orgánica de Protección de Datos (LOPD), tras la entrada en vigor del Reglamento europeo en mes de mayo.

Los trabajos, que deberán estar concluidos el año que viene, se realizarán en el seno de la Sección Tercera, de Derecho Público de la Comisión General de Codificación, que preside el catedrático de Derecho Administrativo José Luis Piñar.

Estos trabajos son fruto de lo que Aurea Roldán calificó como "un reglamento con alma de directiva, que ha venido a modernizar una legislación que databa de los años 90 y que necesita un importante desarrollo normativo en cada uno de los Estados".

Destacó que el Reglamento da carta de naturaleza a la figura del *compliance officer*, "que es uno de los elementos fundamentales de compromiso de las empresas para el cumplimiento de esta norma".

En busca de una constancia inequívoca

Uno de los asuntos fundamentales del periodo transitorio es el de la modificación en la forma de recoger el consentimiento de los titulares de los datos que van a ser tratados. El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

Esto podría incluir marcar una casilla de un sitio web en Internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no constituyen consentimiento y éste debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines.

Desequilibrios entre las partes

Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en el caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.

Se presume que no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.

Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos y cada uno de ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios elec-

[CONTINÚA]

Catalá dice que el nuevo Reglamento puede ser considerado como “el principal hito en esta materia en los últimos años”

El silencio, las casillas ya marcadas en la web o la inacción no constituyen consentimiento del titular de los datos

Se presumirá que no se ha dado libremente cuando no se permita autorizar por separado cada operación de tratamiento

El ‘big data’ -tratamiento masivo- afecta a todos los sectores económicos y tiene grandes implicaciones en la privacidad

trónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, en estos casos, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

En su intervención en la jornada de la Cátedra Google, Ángels Barbará, directora de la Autoridad Catalana de Protección de Datos, analizó el paso que supone el nuevo Reglamento “desde un estándar mínimo de medidas de seguridad en el Reglamento a una obligación de análisis de riesgos, lo que permite ir adaptando la defensa de la persona a los adelantos tecnológicos que se vayan produciendo en cada momento”.

Avisó a quienes suben fotografías de grupos de personas a las redes sociales, que los cambios en la normativa comunitaria incluyen la responsabilidad ante las denuncias que se le puedan presentar por ello. “Se ha dado un cambio de concepto, ya que hasta ahora era una cuestión formal, sin trascendencia, pero que ahora requiere de la aceptación explícita de todos y cada uno de lo reflejados en la foto”, añadió.

Así, las compañías de *headhunters* -caza talentos- aparte de tener en cuenta el currículo, revisan las redes sociales. “Imagínense si después de una noche loca en el lugar de veraneo alguien sube una foto a una red social en la que usted está en una actitud no muy digna. Estas empresas descartan a los candidatos por conductas que consideran reprobables”.

También se exigirá la autorización de los padres para subir las fotos de los grupos de alumnos de los colegios y en el caso de los teléfonos móviles, ya no podrán venir activadas todas las aplicaciones, con la autorización tácita, sino que el usuario deberá instalarlas una a una y dando su aceptación explícita.

Autoridades públicas en misión oficial

Esta protección, sin embargo, no existe cuando es a las autoridades públicas a las que se comunican los datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros.

No obstante, esta solicitud de comunicación por las autoridades públicas tiene también sus limitaciones, puesto que siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no han de referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

‘Big data’ e innovación tecnológica

A pesar de los controles sobre el *big data* -el tratamiento masivo de datos, que introduce el Reglamento, José Luis Piñar -titular de la Cátedra Google- explicó que “no va a impedir la innovación tecnológica, sino que lo que se pretende es marcar el camino por donde deben ir esos avances técnicos, y, por eso, técnicos y juristas deben ir de la mano en su desarrollo y aplicación”.

El *big data* afecta a todos los sectores económicos y tiene grandes implicaciones en la privacidad, por ello, el director de políticas y asuntos públicos de Google, Francisco Ruiz Antón, comentó que para Google, la transparencia y el control de los datos por parte de los usuarios es un principio fundamental. Por eso ponemos a su disposición herramientas para que sepan qué datos tiene Google y para que puedan decidir qué hacer con ellos”.

El nuevo Reglamento tiene como objetivo el garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la UE. El nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros.

El problema que trata de resolver es que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de Internet, identificadores de sesión en forma de *cookies* u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto deja huellas que al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

Protección específica para los niños hasta cumplir los 16 años

Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños. Cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender. Cuando se realice la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si es menor, tal tratamiento sólo se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Nuevo Reglamento General comunitario

Comienza la cuenta atrás para adaptarse

La Agencia Española de Protección de Datos recomienda a las empresas el inicio de su puesta al día sobre las exigencias que regirán en 2018

XAVIER GIL PECHARROMÁN

La Agencia Española de Protección de Datos (AEPD) recomienda a las empresas y entidades que inicien una adaptación progresiva de sus procesos en materia de protección de datos antes de que comience su aplicación en mayo de 2018, de forma que se puedan detectar las posibles dificultades en su aplicación y tomar medidas que permitan solucionarlas.

"Tenemos un reto importante en los próximos ocho meses, ya que tener preparado un texto de la Ley Orgánica y del Estatuto de la Agencia para marzo del año que viene es un verdadero reto", explicó Mar España, el pasado 29 de junio, en el transcurso de su intervención en la 8ª Sesión Anual Abierta de la AEPD, para explicar que durante este periodo es preciso que las instituciones se vayan preparando con tiempo.

Existe una diferencia fundamental entre el Reglamento europeo y la normativa española actual en lo que al consentimiento se refiere. La norma comunitaria exige una manifestación expresa e inequívoca, lo que supone que se prohíbe el consentimiento tácito, que era una de las fórmulas más utilizadas por las empresas.

Por ello, su texto regula que los consentimientos obtenidos con anterioridad seguirán siendo válidos si se obtuvieron respetando los criterios establecidos por esta normativa comunitaria.

Así las cosas, Mar España (en la foto) recomendaba que las organizaciones que basen sus consentimientos en fórmulas tácitas, que empiecen ya a adaptarse a las exigencias del Reglamento.

N. MARTÍN

Cláusulas informativas

Otra importante diferencia se refiere a la información que debe facilitarse a los interesados con anterioridad al inicio de los tratamientos, el Reglamento incluye cuestiones adicionales que aún no han sido requeridas por la normativa española. Así, las cláusulas informativas utilizadas con anterioridad a mayo de 2018, deberían recibir una adaptación progresiva por varias vías.

"Por una parte, muchas organizaciones pueden proporcionar esa información adicional sin costes o esfuerzos excesivos utilizando para ello sus páginas web o aprovechando los canales de comunicación regulares que puedan mantener con sus clientes. Estas buenas prácticas contribuirían a reducir el número de casos en que las cláusulas informativas presenten carencias cuando el Reglamento sea de aplicación", explicó Mar España.

Al mismo tiempo, es aconsejable que las organizaciones adapten sus políticas informativas a lo dispuesto por el Reglamento. Hay algunas cuestiones donde esa información dependerá de la adopción de otras decisiones, como puede ser el proporcionar los datos del delegado de Protección de Datos.

Esos datos no podrán trasladarse a los interesados hasta que ese delegado no sea designado en los casos en que el Reglamento lo hace obligatorio o cuando las organizaciones decidan voluntariamente nombrarlo, pero otros elementos sí pueden ya anticiparse y, en la medida de lo posible, incorporarse sin dilación a las informaciones que se proporcionan a los interesados.

Es por ello, que la AEPD estima que en estos casos no será necesario comunicar la cláusula informativa a todas aquellas personas sobre las que ya se está realizando el tratamiento, sino que bastará con publicarlas en la página web de la empresa o institución, o a través de los canales de comunicación habituales que puedan mantener con sus clientes. Recomienda, a este respecto, que se vayan adaptando las cláusulas informativas con tiempo las exigencias del Reglamento.

Evaluaciones de Impacto

La realización de Evaluaciones de Impacto sobre la protección de datos -aplicables de forma obligatoria en ciertos tratamientos- tiene carácter previo a la puesta en marcha de los mismos y tiene como objetivo minimizar los riesgos que un tratamiento de datos plantea para los ciudadanos. La realización de estas Evaluaciones tiene carácter previo a la puesta en marcha de los correspondientes tratamientos.

Por ello, Mar España explicó que "posiblemente no sería acorde con el espíritu del Reglamento exigir que todo tratamiento que pueda potencialmente suponer un alto riesgo para los derechos de los interesados deba ser objeto de una Evaluación de Impacto, pese a haber comenzado antes de que resulte aplicable".

La Agencia considera que no debería esperarse a la fecha en que la realización de las evaluaciones resulte obligatoria para comenzar a utilizar esta herramienta, ya que requiere de preparación, elección de la metodología adecuada, identificación de los equipos de trabajo y otra serie de condiciones que no pueden improvisarse. Comenzar a incorporar este sistema a la actuación de las organizaciones no sólo les permitirá estar en mejores condiciones en el momento en que resulte obligatorio para algunas de ellas, sino que también les permitirá asegurar el cumplimiento no ya del futuro Reglamento, sino incluso de la actual normativa.

Esquemas de certificación

El Reglamento concede una atención especial a la implantación de esquemas de certificación y abre diversas posibilidades para su gestión. Las certificaciones pueden ser otorgadas por las autoridades de protección de datos, tanto individual como colectivamente desde el Comité

[CONTINÚA]

Se prohibirá el consentimiento tácito, que es una de las fórmulas más utilizadas por las empresas hasta ahora

Resulta aconsejable que las organizaciones adapten sus políticas informativas a lo dispuesto por el Reglamento

Las pymes dispondrán de herramientas que ayuden a responsables y encargados a entender y cumplir la norma

Los delegados de protección de datos serán nombrados por las empresas en función de sus cualificaciones profesionales

Europeo, o por entidades debidamente acreditadas. Al mismo tiempo, en el caso de optarse por esta última alternativa, la acreditación pueden llevarla a cabo las propias autoridades o encargarlo a las entidades de acreditación previstas en la normativa europea sobre normalización y certificación. En todo caso, en la elaboración de los criterios tanto para acreditar entidades como para certificar a las organizaciones, tienen diferentes grados de participación las autoridades de supervisión y el Comité Europeo.

Mar España advirtió que la AEPD entiende que, de entre estas posibilidades, la que mejor responderá a las necesidades de las entidades al tiempo que es compatible con la configuración y posibilidades de actuación de la Agencia es la de encomendar la certificación a entidades especializadas debidamente acreditadas y dejar que se ocupe de la acreditación de éstas la Entidad Nacional de Acreditación (ENAC), contando para ello con la participación de la Agencia.

Cualificación de los delegados

Como en todos los procedimientos administrativos en los que se crea un nuevo tipo de especialistas, la titulación se convierte en unos de los caballos de batalla entre los distintos colectivos profesionales que aspiran a copar los puestos.

En este aspecto, el nuevo Reglamento requiere que los delegados de protección de datos (DPD) sean nombrados en función de sus cualificaciones profesionales, en especial su conocimiento en materia de protección de datos, y su capacidad para el desempeño de sus funciones.

Sin embargo, no establece específicamente cuáles han de ser esas cualificaciones profesionales ni tampoco el modo en que podrán demostrarse ante las organizaciones que deban incorporar esta figura. De hecho, el Reglamento indica en uno de sus considerandos que la valoración de estas aptitudes y conocimientos deberá realizarse no tanto en función de criterios externos como de las necesidades de los tratamientos concretos que cada organización lleve a cabo.

"La Agencia considera que no es oportuno establecer un sistema de certificación de Delegados de Protección de Datos que opere como requisito para el acceso a la profesión", advirtió su directora en la 8ª Sesión Anual Abierta de la AEPD.

En la actualidad, ya existe una oferta de certificaciones y titulaciones que respaldan conocimientos, experiencia o práctica en el ámbito de la protección de datos. Esas titulaciones están llamadas a jugar un papel relevante en el desarrollo de las profesiones relacionadas con la protección de datos en la medida en que pueden servir como un elemento más, aunque no sea necesariamente único, para que la organización que tiene que designar un DPD pueda tener constancia de la formación o cualificaciones de los posibles candidatos.

Y Mar España añadió que "para que la oferta de certificaciones y titulaciones funcione de manera rigurosa es necesario que estas reúnan unos requisitos que permitan que las entidades que los reciban puedan tener un razonable grado de certeza sobre lo que reflejan".

Acreditación de las certificaciones

La Agencia está valorando la posibilidad de promover la aplicación de la acreditación de entidades de certificación de profesionales con arreglo a estándares ya establecidos. Esta acreditación, que llevaría a cabo la Entidad Nacional de Acreditación (ENAC) de acuerdo con lo previsto en esos estándares y con las peculiaridades propias del sector, serviría para constatar que la entidad que expide los títulos, certificados o certificaciones lo hace con arreglo a unos determinados procedimientos y requisitos. La acreditación no se pronuncia sobre la calidad de los contenidos de la formación o de los aspectos que se certifican.

No obstante, matizó Mar España que "el hecho de que algunas entidades se acrediten no implicará necesariamente que otras que no lo hagan no puedan aplicar los mismos criterios ni tampoco que la posesión de la titulación o certificación sea la única vía que permita acceder a un puesto de DPD".

La Agencia considera que estas cuestiones tendrían un carácter instrumental orientado a ofrecer apoyo a las organizaciones a la hora de designar a un DPD.

No obstante, en ningún caso excluyen que profesionales con formaciones procedentes de centros no acreditados o sin una formación específica, pero con experiencia profesional puedan desempeñar las funciones de delegado si su currículo muestra que reúnen los requisitos de conocimiento y cualidades profesionales que el Reglamento establece.

Herramientas para pymes

Finalmente, la directora de la Agencia de Protección de Datos informó de que la Agencia trabaja en la actualidad en la preparación de herramientas que ayuden a responsables y encargados al entendimiento y cumplimiento del Reglamento.

Entre ellas, destaca un recurso *online* orientado a las pymes que realicen tratamientos de bajo o muy bajo riesgo, de forma que puedan constatar de una manera sencilla que se encuentran en esa situación y, a la vez, disponer de una lista de las medidas a implantar en función de ese bajo nivel de riesgo. Está previsto que este recurso se complemente con otros más avanzados, orientados a las pymes que desarrollan tratamientos que conllevan un nivel de riesgo algo mayor como consecuencia de alguna circunstancia concreta -como puede ser el manejo de datos sensibles- y que incluirá un apartado dedicado a las medidas de seguridad que deben implantarse.

La AEPD está trabajando junto a las agencias autonómicas en cláusulas informativas adaptadas al nuevo Reglamento para sectores o tratamientos diferenciados. Así, está previsto ofrecer una serie de recomendaciones o criterios para ayudar a reflejar los distintos puntos que el Reglamento exige en la información.

El departamento de admisión a trámite de las denuncias

La Agencia Española de Protección de Datos (AEPD) ha puesto en marcha un departamento de admisión a trámite para aligerar los tiempos de gestión -15 días-, que absorberá en torno al 50 por ciento de las denuncias que realizan los ciudadanos cada año, en los casos en que no se cumplen todos los requisitos o se comprueba que no viola la norma. Entre las previsiones de la AEPD se prevé abordar el desarrollo del registro electrónico y a generalizar la firma electrónica, la comparecencia voluntaria en sede electrónica para las personas jurídicas y determinados colectivos de personas físicas, como los colegios profesionales, la dirección habilitada única, la notificación y el expediente electrónicos. Por otra parte, la AEPD está elaborando una serie de guías como la de 'Privacidad y Seguridad en Internet', la de 'Buenas Prácticas de Protección de Datos en Proyectos Big Data', así como material audiovisual sobre la privacidad en las redes sociales. También, según explica Emilio Aced, coordinador de la Unidad de Evaluación y Estudios Tecnológicos de la AEPD se está desarrollando un estudio sobre reutilización de material sanitario, así como evaluaciones de impacto sobre los contadores inteligentes.

Nuevo Reglamento General comunitario

“La norma busca prevenir y no solo cumplir”

Rafael García Gozalo, responsable del Área Internacional de la AEPD, analiza algunos de los aspectos claves de la normativa comunitaria

XAVIER GI PECHARROMÁN

El Reglamento Europeo de Protección de Datos prevé que los responsables del tratamiento deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de acuerdo con la propia norma.

Para Rafael García Gozalo, responsable del Área Internacional de la Agencia de Protección de Datos (AEPD), se trata de prevenir. Así, asegura que “no se trata de cumplir razonablemente la norma para evitar la sanción, sino que lo que el Reglamento prevé son cinco o seis grandes ejes de medidas, que efectivamente hay que cumplir, pero no es el objetivo en sí mismo. Hay que cumplirlas, porque si tú las cumples estarás en condiciones de evitar la infracción, evitar tratar más datos de los debidos, evitar quiebras de seguridad, que inconscientemente estés cediendo datos a quien no debes y cosas similares. Es decir, hablamos de *compliance* en el mismo sentido que se puede hablar en otras áreas, pero me gusta lanzar el mensaje de que con el Reglamento hay que ir más allá”.

Así, los códigos de conducta facilitan la correcta aplicación del Reglamento, teniendo en cuenta las características específicas de los distintos sectores y las necesidades específicas de las pequeñas y medianas empresas (pymes). Además, aportan garantías para las transferencias internacionales de datos. Las Agencias de Protección de Datos están obligados a impulsarlos.

Estos códigos servirán de elemento para demostrar el cumplimiento de las obligaciones del responsable. El cumplimiento de los códigos se tendrá en cuenta a efectos de evaluar el impacto de protección de datos de las operaciones de tratamiento (Pias). Podrá servir también de elemento para demostrar el cumplimiento de las obligaciones sobre medidas de seguridad y que el encargado adherido a un código ofrece garantías sensibles. Aunque no sea decisivo, se tendrá en cuenta a la hora de dictaminar las sanciones. Y el control de cumplimiento del código podrá ser llevado a cabo por un organismo con el nivel de pericia adecuado en relación con el código y que haya sido acreditado por la AEPD.

“El Reglamento considera insuficiente cumplir e incluye obligaciones dirigidas a prevenir los incumplimientos. Sin olvidar que la consecuencia de no aplicar estas medidas son las sanciones. Así, exige la aplicación de medidas técnicas y organizativas adecuadas y el tratamiento por defecto”, explica García Gozalo.

EE

Delegado de protección de datos

El nuevo Reglamento introduce una serie de medidas que es necesario tener en cuenta a la hora de adoptar medidas preventivas. Entre ellas destaca el registro de actividades; las medidas de protección de datos desde el diseño y por defecto; las medidas de seguridad adecuadas; las evaluaciones de impacto; la evaluación previa o las consultas con la AEPD; el delegado de protección de datos; la notificación de quiebras de seguridad; y los códigos de conducta y esquemas de certificación.

La adhesión a un código de conducta a un mecanismo de certificación podrá servir de elemento para demostrar cumplimiento, puesto que el Reglamento no establece un listado estructurado de medidas.

Con respecto a la figura del delegado de protección de datos (DPD), el Reglamento prevé que no tendrá que ser obligatorio el designarlo para todas las empresas e instituciones, sino que “se ha optado por una posición de equilibrio entre la introducción de esta medida, que persigue que determinadas organizaciones tengan que contar necesariamente con un asesoramiento experto en la actividad de protección de datos y, como factor de proporcionalidad, de que no todas las empresas se van a beneficiar de la existencia del DPD”, explica Rafael García Gozalo.

Como gran novedad -explica- será obligatorio en la Administración Pública por el tipo de tratamiento y la cantidad de datos que maneja, especialmente sensibles. También, lo será en las empresas que realicen tratamientos de datos a gran escala, que manejen datos sensibles o que realicen una monitorización habitual de la conducta de los interesados.

Comenta también que “esta división, no obstante, no quiere decir que las demás empresas no puedan contar con asesoramiento en protección de datos, al igual que tienen asesoramiento experto en fiscalidad o en riesgos laborales”.

Las principales misiones del delegado son las de informar y asesorar a la organización en todos los temas relacionados con protección de datos, y, por otro lado, tiene unas funciones internas de supervisión de las medidas que permitirán a la organización estar en condiciones de cumplir con lo que el Reglamento prevé. Una de las cosas que el delegado tiene que realizar es la supervisión de los programas de formación en materia de protección de datos dentro de una organización.

Añade García Gozalo que “desde la perspectiva de la AEPD es un factor positivo. Pensamos que más allá de la obligación que establece el Reglamento, esta figura puede ser muy útil, pero no se puede focalizar la atención en esta medida sobre el resto de las incluidas en el Reglamento. No se puede aislar la figura del DPD. El Reglamento prevé un paquete de medidas que funcionan de forma integrada”.

La existencia de un DPD tiene sentido en sí misma, pero más si se conjuga con la necesidad de adoptar medidas de privacidad de protección de datos desde el diseño, con las evaluaciones

[CONTINÚA]

“Hablamos de ‘compliance’ en el mismo sentido que se puede hablar en otras áreas, pero hay que ir más allá”

“La introducción del delegado persigue que determinadas organizaciones cuenten con un asesoramiento experto”

“Esa forma de consentimiento, que llamamos tácito, es una situación muy peculiar en España”

“Se incluyen medidas negativas de discriminación, que son una continuación reforzada de lo que ya preveía la Directiva”

de impacto para determinados tratamientos, con la necesidad de mantener un registro o una información detallada sobre todos los tratamientos que realiza la organización. Todas esas medidas se refuerzan entre sí. “De hecho, el DPD tiene mucho que ver en todas ellas”, concluye.

Consentimiento

El Reglamento es muy claro en sus términos al referirse al consentimiento del interesado para el tratamiento de los datos. Exige su vinculación a uno o varios fines específicos. Debe ser inteligible, accesible y en lenguaje claro y sencillo. El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

En caso de declaración escrita debe quedar claramente diferenciada de otras declaraciones distintas. Además, debe ser revocable con la misma facilidad dada para prestarlo. Debe asumirse libremente por el titular de los datos y la carga de la prueba corre a cargo del responsable. Queda eliminado el consentimiento tácito.

“Esa forma de consentimiento, que llamamos tácito, es una situación muy peculiar en España. Creo que esto debiéramos empezar a planteárnoslo, porque esto se incluyó en la normativa por diversas razones y ha funcionado hasta ahora, pero es una rareza en el contexto de los demás Estados de la UE”, explica el responsable del Área Internacional de la AEPD.

No hay figuras paralelas en otros Estados. Históricamente nuestra legislación no preveía la posibilidad de tratar los datos sobre la base del interés legítimo de quien trata los datos, más que en unos casos muy concretos y limitados, y ante la imposibilidad de hacer los tratamientos sobre esa base legal, que es la que se empleaba en otros países, pues aquí se desarrolló esta figura del consentimiento tácito.

Además -señala-, desde la emisión de la sentencia del Tribunal de Justicia de la UE (TJUE), de 24 de noviembre de 2011, esta posibilidad de utilizar el interés legítimo también se aplica en España, ya hay empresas que han empezado a recurrir a él en lugar de tener que andar basándose en este consentimiento tácito, que no deja de ser una rareza”.

Por tanto, indica García Gonzalo, “ya tenemos empresas que no se van a ver en esa situación de tener que actualizar sus consentimientos tácitos, por lo que se disminuye el efecto de esta novedad, que ya han pasado unos años para que determinadas empresas hayan recurrido ya a esto. No obstante, todavía quedan empresas que siguen basando sus tratamientos en el consentimiento tácito y, además, con un número importante de afectados. Y lo cierto es que el Reglamento no deja mucho margen de interpretación ni de maniobra. Esos tratamientos tienen que encontrar una base legal de acuerdo con el Reglamento y no pueden seguir basándose en el consentimiento tácito a partir de mayo de 2018”.

Por ello, estas empresas deben empezar desde ya, para ir haciéndolo paulatinamente, porque eso va a ayudar a reducir el impacto de los costes de esa operación. Muchas de estas compañías tienen un contacto regular con sus clientes o estos consentimientos tácitos van más allá del que vincula a una empresa con sus clientes.

“En muchos casos, a través de la relación regular con los clientes, se puede recabar el consentimiento inequívoco, que es lo que exige el Reglamento, sin unos costes excesivos. Si se opta por alguna otra base legal hay que formalizarlo y formar a los interesados, entre otras cosas. No es un proceso de reflexión interna de la organización, sino que hay que realizar una serie de trámites”, explica García Gozalo.

Discriminación

Uno de los principales problemas que se plantean son las posibilidades de discriminación que pueden surgir del tratamiento de datos.

A este respecto, García Gozalo explica que “el Reglamento es muy consciente de las posibilidades de discriminación que puede conllevar el tratamiento de datos; por ello, incluye medidas negativas de discriminación, que son una continuación reforzada de lo que ya preveía la Directiva, puesto que en ambos casos se abordan desde el punto de vista de dato sensible, de dato especialmente protegido”.

Entre estos datos sensibles se encuentran los referidos a salud, raza, religión, opiniones políticas y preferencias sexuales. Incluso, el Reglamento incluye algunos nuevos como los genéticos y los biométricos, con lo que se trata de impedir que estos datos sean tratados para impedir que se pueda identificar a las personas. “Estos datos son los que están más relacionados con la esfera de su privacidad, de su intimidad. Si se tratan inadecuadamente pueden dar lugar a discriminación y, por ello, hay una prohibición de tratar esos datos como norma de partida”, señala García Gozalo.

Sin embargo -añade-, existen una serie de excepciones en las que la presencia de otros intereses de alta calidad hace posible que se puedan tratar. En la mayoría de esas excepciones tiene que mediar una norma de los Estados miembros de la Unión Europea que determine en qué condiciones se pueden tratar, como garantía adicional.

García Gozalo concluye señalando que “también hay medidas positivas contra la discriminación, como las que tienen que ver con los menores para quienes también hay unas garantías reforzadas, sobre todo en el ámbito de los servicios de la sociedad de la información, donde están prácticamente todos. Se trata de un ámbito donde los menores pueden estar más desprotegidos. Cuando un menor está en un ordenador no se sabe si está su padre con él o qué edad tiene. Por ello, están reguladas estas garantías adicionales”.

La investigación científica debe respetar las normas éticas

Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida. Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente. Entre los datos personales relativos a la salud se deben incluir todos los relativos al estado de salud del interesado pasado, presente o futuro.

Nuevo Reglamento General comunitario

Evitar que las personas sean identificadas

Las personas físicas deben tener conocimiento de los riesgos, normas, salvaguardias y los derechos relativos al tratamiento de datos personales

XAVIER GIL PECHARROMÁN

El nuevo Reglamento supone una garantía adicional a los ciudadanos europeos. En la actualidad, para tratar datos no es necesario mantener una presencia física sobre un territorio, por lo que el Reglamento pretende adaptar los criterios que determinan qué empresas deben cumplirlo a la realidad del mundo de Internet.

Ello permite que el Reglamento sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión y, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea.

El problema que trata de resolverse es que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de Internet, identificadores de sesión en forma de 'cookies' u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto deja huellas que al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

GETTY

Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. Introduce nuevos elementos, como el *derecho al olvido* y el *derecho a la portabilidad*, que mejoran la capacidad de decisión y control de los ciudadanos sobre los datos personales que confían a terceros.

El *derecho a la portabilidad* implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá transferir los datos directamente al nuevo responsable designado por el interesado.

El 'derecho al olvido'

El *derecho al olvido* se presenta como la consecuencia del derecho que tienen los ciudadanos a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.

Asimismo, según la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que reconoció por primera vez el *derecho al olvido* recogido ahora en el Reglamento europeo, supone que el interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público, entre otros motivos.

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento deben ser explícitos y legítimos, y deben determinarse en la recogida.

Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales sólo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

Para garantizar que el consentimiento se ha dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando el responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.

Constancia de que se efectúa la recogida

Se presume que el consentimiento no se ha dado libremente cuando no permite autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para el cumplimiento.

[CONTINÚA]

Los derechos al 'olvido' y a la 'portabilidad' mejoran la capacidad de decidir y el control de datos a los ciudadanos

Los fines específicos del tratamiento deben ser explícitos y legítimos, y deben determinarse en la recogida

Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

Este principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.

Algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya existentes, como es el caso de las medidas de seguridad o de la obligación de documentación y, hasta cierto punto, la evaluación de impacto y la consulta a Autoridades de supervisión.

Otras constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que formarían parte de una correcta puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto, la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos.

Factores de riesgo

El Reglamento prevé que la obligación de estas medidas, o el modo en que se apliquen, dependerá de factores como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos. Por ello, es preciso que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para determinar qué medidas han de aplicar y cómo hacerlo.

Estos análisis pueden ser operaciones muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen datos sensibles, u operaciones más complejas en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que, por sus características, requieran de una valoración cuidadosa de sus riesgos.

El Reglamento prevé que se incluyan en la información que se proporciona a los interesados una serie de cuestiones que con la Directiva y muchas leyes nacionales de transposición no eran necesariamente obligatorias. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados puedan dirigir sus reclamaciones a las Autoridades de protección de datos. Este sistema está pensado para que los responsables establecidos en varios Estados miembros o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE, tengan una única Autoridad de protección de datos como interlocutora.

La norma se aplica a los tribunales fuera de su función jurisdiccional

El Reglamento europeo se aplica a las actividades de los tribunales y otras autoridades judiciales, aunque no en el ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento del Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos. La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El Reglamento no se aplica, por lo tanto, a las actividades de tratamiento destinadas a tales fines. La protección ante amenazas a la seguridad pública y su prevención, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del Reglamento.

La aplicación de las medidas depende del tipo de tratamiento, costes de implantación de las medidas o riesgo

Si se presentan discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos

Un nuevo sistema transfronterizo

También implica que cada Autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, a partir de la aplicación del Reglamento valorará si el supuesto tiene carácter transfronterizo, en cuyo caso habrá que abrir un procedimiento de cooperación entre todas las Autoridades afectadas buscando una solución aceptable para todas ellas.

Si hay discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos, un organismo de la Unión integrado por los directores de todas las Autoridades de protección de datos de la Unión. Ese Comité resolverá la controversia mediante decisiones vinculantes para las Autoridades implicadas.

Este nuevo sistema no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades distintas de la del Estado donde residan.

Siempre pueden plantear sus reclamaciones o denuncias ante su propia Autoridad nacional -en el caso español, la AEPD-. La gestión será realizada por esa Autoridad, que será también responsable de informar al interesado del resultado final de su reclamación o denuncia.

La *ventanilla única*, en todo caso, no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado.

En general, las organizaciones que tratan datos personales deberían comenzar a preparar la aplicación de estas medidas, así como de otras modificaciones prácticas derivadas del Reglamento. Por ejemplo, el Reglamento exige que los responsables de tratamiento faciliten a los interesados el ejercicio de sus derechos. Aunque la interpretación de *facilitar* pueda variar dependiendo de los casos, incluye en todos ellos algún tipo de actuación positiva por los responsables para hacer más accesibles y sencillas las vías para el ejercicio de derechos.

La ventaja de una pronta aplicación es que permitirá detectar dificultades, insuficiencias o errores en una etapa en que estas medidas no son obligatorias y, en consecuencia, su corrección o eficacia no estarían sometidas a supervisión. Ello permitiría corregir errores para el momento en que el Reglamento sea de aplicación.

La salud y la infancia reciben un tratamiento especial ampliado

XAVIER GIL PECHARROMÁN

Se incluyen todos los datos que dan información sobre el estado de salud física o mental pasado, presente o futuro

Cuenta con la información de pruebas o exámenes de una parte del cuerpo o sustancia corporal y datos genéticos

Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, en estos casos, el nuevo Reglamento Europeo de Protección de Datos establece que debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas.

Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida. A este respecto, señala el nuevo Reglamento comunitario, que debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier elemento que permita obtener información similar.

Regula también el Reglamento que entre los datos personales relativos a la salud se deben incluir todos los relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia.

ISTOCK

Caracteres identificativos

De esta forma, se considera todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios.

También se incluye en la regulación la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente; por ejemplo, un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in *vitro*.

Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto.

Regula el Reglamento que el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas.

Razones de interés público

En ese contexto, salud pública se interpreta en la definición del Reglamento 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad.

Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

Protección especial infantil

Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales.

Dicha protección específica debe aplicarse, en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño.

El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

Este principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.

La Agencia Española de Protección de Datos deberá adaptar su Estatuto

El nuevo Reglamento y la Directiva son considerados por los técnicos de la AEPD como determinantes en su actividad

Deberá analizar los impactos sectoriales y sobre colectivos de interesados, en colaboración con las entidades representativas

XAVIER GIL PECHARROMÁN

La Agencia Española de Protección de Datos (AEPD) presentó en noviembre de 2015 su Plan Estratégico 2015-2019, tras haber recibido en la fase de consulta pública casi 400 aportaciones ciudadanas, responsables de tratamiento, expertos y organizaciones públicas y privadas, que se propone dar respuesta a los retos internacionales, especialmente ante la próxima aprobación del nuevo Reglamento Europeo de Protección de Datos, que obligará a replantearse el Estatuto Orgánico de la Agencia para adaptarlo a las nuevas exigencias.

Indica el Reglamento, que desde la perspectiva de responsables y encargados de tratamiento, quizás el aspecto más relevante sea la introducción de un principio general de *accountability* -responsabilidad activa-.

Prevé, asimismo, que los responsables y encargados establezcan mecanismos que les coloquen en situación de poder cumplir con los principios y derechos que en él se prevén. Deben, además, estar en condiciones de poder demostrar que disponen de esos mecanismos y que su adopción se adecúa a los riesgos que los tratamientos que realizan conllevan.

Cooperación entre Administraciones

Para las autoridades de protección de datos la gran novedad del Reglamento, aparte de algunas que ya existían en el ordenamiento, como la atribución de potestad sancionadora, es la intensa cooperación entre autoridades que deberá presidir el ejercicio de sus funciones.

Señala la AEPD en su Plan el llamado sistema de 'ventanilla única' para responsables y ciudadanos, el mecanismo de coherencia y las diversas modalidades de cooperación, que incluyen la posibilidad de realizar inspecciones conjuntas, dibujan un panorama en que muchas de las decisiones, tanto singulares respecto a casos concretos como generales en su papel de asesoramiento en la interpretación y cumplimiento de las normas, se tomarán en procesos de decisión colectivos. La mejor expresión de esta nueva orientación es el futuro Consejo Europeo de Protección de Datos, que según alguna de las propuestas que manejan los colegisladores europeos podría convertirse en un organismo de la UE.

El nuevo Reglamento, y en menor medida la futura Directiva, son considerados por los técnicos de la AEPD como determinantes en su actividad. Por una parte, deberá valorar los contenidos del Reglamento con vistas a sensibilizar y asesorar tanto a las autoridades con potestades normativas como a las empresas, las instituciones y los ciudadanos.

En ese mismo sentido, deberá determinar qué actuaciones propias pueden ser necesarias para una correcta aplicación del Reglamento y establecer las necesarias prioridades para su puesta en marcha. Esa tarea, por otro lado, no se limita al ámbito interno sino que debe desarrollarse también, paralelamente, en el plano europeo, donde el Grupo de Autoridades europeas de Protección de Datos prevé un programa de trabajo en la misma línea. Y, además, la Agencia deberá analizar los cambios que será necesario introducir en su estructura y procesos para adecuarse a los nuevos métodos de funcionamiento impuestos por el nuevo Reglamento comunitario.


EE

La AEPD se plantea la exhaustiva misión de analizar los contenidos del Reglamento y su impacto en la vigente normativa de protección de datos, comenzando por la LOPD y su Reglamento de desarrollo, con la finalidad de asesorar a las diversas autoridades del Estado y Comunidades Autónomas que puedan verse afectadas y cooperar con ellas en la identificación de disposiciones que serán desplazadas por el Reglamento, en la identificación y desarrollo de posibles modificaciones o adaptaciones que deban llevar a cabo los Estados miembros, y en la identificación y preparación de las medidas interpretativas, directrices o buenas prácticas que la AEPD debiera aprobar.

En esta tarea, la Agencia debe además analizar impactos sectoriales y sobre colectivos de interesados, en colaboración con entidades representativas de sectores empresariales, organizaciones ciudadanas y profesionales de la privacidad. Asimismo, la AEPD evaluará los efectos del Reglamento sobre sus distintas actividades para diseñar y poner en práctica las necesarias adaptaciones estructurales y procedimentales.

Finalmente, la Agencia debe desarrollar las actuaciones necesarias para participar eficazmente en los trabajos orientados a la aplicación del Reglamento a nivel europeo, en particular dentro del Grupo de Autoridades del Artículo 29, cuyo programa de trabajo 2016-2018 está centrado en el proceso de transición al futuro Consejo Europeo de Protección de Datos y en la preparación de las primeras directrices o criterios que el Reglamento atribuye al futuro Consejo.

La AEPD tiene también la misión de promover el análisis de las novedades que incluye la nueva Directiva para determinar su impacto en la vigente normativa a los efectos de asesorar y sensibilizar a las autoridades con competencias legislativas sobre las medidas a adoptar, con especial referencia a la posible vigencia de determinadas previsiones de la Ley Orgánica de Protección de Datos (LOPD).

Todos estos esfuerzos se complementan con el Plan de digitalización de la Agencia, en el marco de la colaboración prevista con la Comisión de Estrategia de las Tecnologías de la Información y la Comunicación (TIC) y con otros organismos de la Administración estatal. Además, se prevé para este año dar un impulso del Registro Electrónico como canal de comunicación con la Agencia y la utilización del CL@VE como medio de identificación en la Sede electrónica, entre otras medidas. Para 2017, se prevé la generalización de la firma electrónica en todos los documentos y la extensión de la notificación por comparecencia en Sede a todos los procedimientos.