El Reglamento sobre protección de datos, necesario pero descafeinado

El 25 de mayo entró en vigor el Reglamento europeo 2016/679 sobre protección de datos personales. RED SEGURIDAD organizó un "Sobre la Mesa", con el patrocinio de la Fundación Borredá, donde reunió a cinco especialistas sobre la materia para desgranar el documento. Si bien todos consideraron positiva la aprobación de la nueva norma, no escondieron sus reticencias en torno a algunos de sus contenidos.

Enrique González, redactor jefe de RED SEGURIDAD; Francisco Herráiz, director de TI del Instituto Psiquiátrico José Germain; Rafael Velázquez, consultor legal de TI; Esmeralda Saracíbar, miembro del Comité del Data Privacy Institute de ISMS Forum; Rafael García del Poyo, presidente del Comité Asesor de Eurocloud; Laura Borredá, representante de la Fundación Borredá; Miguel Geijo, secretario de la Asociación Profesional Española de Privacidad; y David Marchal, colaborador de RED SEGURIDAD.

Tx.: David Marchal.
Ft.: RED SEGURIDAD.

CUATRO AÑOS DE INTENSO TRABAJO por parte de las autoridades legisladoras de la Unión Europea han sido necesarios para que haya visto la luz el nuevo 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 los datos personales y a su libre circulación. Un texto que deroga la Directiva 95/46/CE, hasta ese momento en vigor, y establece un periodo de dos años para que su aplicación sea efectiva. Es decir, de aquí al 25 de mayo de 2018, los Estados, las empresas y las Administraciones Públicas deben realizar las modificaciones y ajustes necesarios para garantizar su cumplimiento.

Para intentar comprender las implicaciones que la nueva norma tendrá para los ciudadanos y las organizaciones europeas, RED SEGURIDAD organizó, con el patrocinio de la Fundación Borredá, organizó un "Sobre la mesa" con cinco expertos en la materia. Todos ellos, en sus intervenciones iniciales, constataron la importancia que tiene esta regulación, habida cuenta de que, en palabras de **Esmeralda Saracíbar**, miembro del Comité del Data Privacy Institute del ISMS Forum, "la anterior Directiva databa del año 1995, cuando Internet estaba empezando con un uno por ciento de internautas y no existían tecnologías y servicios hoy en día tan habituales como el *cloud*, los móviles inteligentes o las redes sociales". A lo que añadió: "que se regule todo esto está bien y es un paso más para asegurar la privacidad de los usuarios".

Para **Miguel Geijo**, secretario de la Asociación Profesional Española de Privacidad (APEP), "la directiva anterior estaba obsoleta y generaba problemas para las grandes compañías. Por tanto, era necesaria una nueva norma". Ahora bien, apuntó: "pero tengo mis dudas sobre si regular este tema mediante un reglamento era la manera adecuada". Precisamente, esa idea también generó ciertas dudas en el resto de asistentes. Por ejemplo, **Rafael García del Poyo**, presidente del Comité Asesor de Eurocloud, opinó al respecto: "mi valoración del Reglamento es que

no es ni bueno ni malo, sino lo que toca en estos tiempos. Eso sí, la dificultad radica en saber si ese tipo de normativa era el mejor mecanismo para regularlo". En esa línea se pronunció también **Francisco Herráiz,** director de TI del Instituto Psiquiátrico José Germain: "me parece un buen Reglamento, pero deja muchas cosas en el aire. Cuando entras en el detalle, hay iniciativas importantes que no están bien definidas", comentó. Y a juicio de **Rafael Velázquez**, consultor legal de TI y *Certified Data Privacy Professional* (CDPP), "el Reglamento es claro en muchos aspectos, pero en otros es indeterminado".

El papel de la LOPD

Una de las cuestiones que inmediatamente se puso sobre la mesa fue en qué situación deja esta nueva normativa europea de obligado cumplimiento para los Estados miembros a la Ley Orgánica de Protección de Datos (LOPD) y, consecuentemente, a la Agencia Española de Protección de Datos (AEPD). "No está claro dónde queda la LOPD en relación con el Reglamento", según García del Poyo, de Eurocloud. "No se sabe si será el mecanismo adecuado para regular esto, si se derogará o no", añadió. Geijo, por su parte, no cree que el Reglamento vaya a desplazar a la LOPD, sino que "continuarán ambos", y agregó: "Creo que la LOPD se mantendrá en todo lo que no sea incompatible con el Reglamento".

En cualquier caso, todos los asistentes estuvieron de acuerdo en que España parte con una ventaja respecto a otros países de la UE, puesto que nuestro país tiene una de las legislaciones más avanzadas en protección de datos, con un organismo regulador, como es la AEPD, que ya aplica a las empresas una política estricta de gestión en este ámbito. Según Velázquez, asesor legal de TI, "estamos en el inicio de una nueva aventura en la que países como España tienen todo un histórico consolidado, una forma de entender las cosas y una casuística ya establecida, pero eso no quiere decir que pase lo mismo en el resto de Estados de la UE".

Ahora bien, eso no quita que las empresas españolas no vayan a tener dificultades para implementar esta normativa. Sin ir más lejos, Saracíbar, de ISMS Forum, puso como ejemplo el consentimiento de los usuarios a que las organizaciones almacenen sus datos personales; una cuestión sobre la que el Reglamento "genera una mayor rigurosidad", en tanto en cuanto "acaba con el consentimiento tácito", afirmó. Sin embargo, también suscita dudas. "Si en estos dos años de carencia una empresa ha recabado consentimientos tácitos ¿le sirve o necesitará regularizar consentimientos inequívocos?", se preguntó Saracíbar.

Herráiz, del Instituto Psiquiátrico José Germain, también opinó que "se debería haber ahondado un poco más en el tema del consentimiento, porque las empresas ponen unos textos enormes y los usuarios acaban marcando la casilla por no leérselo todo. Tendrían que haber profundizado más para que,

Esmeralda Saracíbar
Miembro del comité del Data Privacy Institute de ISMS Forum

"El mayor impacto del Reglamento es que ahora el enfoque se basa en riesgos; las empresas deberán aplicar las medidas oportunas en función del riesgo"

Algunos derechos básicos de los ciudadanos

El Reglamento introduce y desarrolla algunos derechos para los ciudadanos que conviene tener en cuenta a la hora de hablar del nuevo marco europeo de protección de datos. Son éstos:

- **Derecho a la rectificación.** Alude al derecho de los usuarios a rectificar los datos personales inexactos que les conciernan, así como la posibilidad de completar otros que se consideren incompletos.
- **Derecho a la supresión ("derecho al olvido").** Permite al interesado obtener sin dilación indebida la supresión de los datos personales que le conciernan, cuando, entre otros, ya no sean necesarios para los fines para los que fueron recogidos, retire su consencimiento, se oponga al tratamiento de los datos, se haya tratado esa información ilícitamente, o deban suprimirse para el cumplimiento de una obligación legal establecida.
- **Derecho a la limitación del tratamiento.** Se hará efectivo cuando, entre otros, se cumpla que el interesado impugne la exactitud de los datos personales; el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; o el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- **Derecho a la portabilidad de los datos.** Habilita el derecho del interesado a recibir sus datos personales, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica.
- **Derecho de oposición.** Da al interesado el derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de tratamiento.

Miguel Geijo
Secretario de la Asociación Profesional Española de Privacidad (APEP)

"Lo que quiere la UE con este Reglamento es que la privacidad se incruste por completo en todas las organizaciones y Administraciones públicas europeas"

cuando demos nuestro consentimiento, estemos seguros de ello".

Responsabilidades empresariales

Pero más allá de temas tan específicos como éstos, lo cierto es que el papel que dibuja el nuevo Reglamento con respecto a las organizaciones es radicalmente distinto al que tenían hasta este momento, tal y como se encargaron de recordar los asistentes a la mesa redonda. "El mayor impacto que genera el Reglamento es que ahora el enfoque se basa en riesgos", explicó Saracíbar. Es decir, "a partir de este momento, las empresas deberán aplicar las medidas que consideren oportunas en función del riesgo. Luego eso evolucionará hacia una evaluación del impacto para la privacidad", añadió.

Lo que viene a decir el legislador a las organizaciones es, en opinión de García del Poyo, de Eurocloud, que busquen un experto que les ayude. "Ésta es la gran revolución, no para nosotros, que estamos acostumbrados a ello por nuestra legislación, sino para el resto de Europa; y especialmente para las compañías norteamericanas, que no han oído hablar nada de esto", matizó.

Velázquez, asesor legal de TI, abundó sobre este tema también: "el Reglamento pasa a un enfoque en el que se busca realizar análisis de riesgos y, según eso, plantear medidas técnicas y organizativas en las compañías". Y eso, a su juicio, implica "una revolución favorable y pensar antes", lo que debe dar lugar a "un cambio de mentalidad importante en las organizaciones".

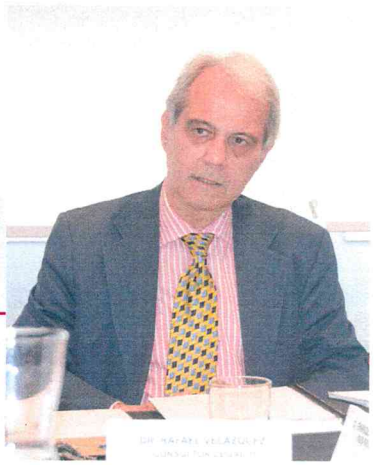
Para García del Poyo, de Eurocloud, esta nueva normativa lo que hace es "cargar sobre los hombros de las empresas" la responsabilidad a la hora de establecer un correcto tratamiento de la gestión de datos e implantar medidas para que no puedan resultar vulnerados. "Eso precisamente es lo que buscan los principios de protección por diseño y por defecto a los que hace referencia el Reglamento", añadió. Por tanto, contar con alguna empresa auditora externa que certifique la correcta aplicación de la norma "va a resultar fundamental a la hora de atenuar o eximir las responsabilidades de las compañías en la imposición de cualquier sanción", en palabras de García del Poyo. En este contexto, "se trata de que las organizaciones se armen de todo tipo de argumentos para, posteriormente, poder defenderse, sin limitar la responsabilidad final que puedan tener", añadió.

Esto, además, lleva implícitas nuevas sanciones mucho más agresivas que las que estábamos acostumbrados en España. "A la hora de hacer el análisis de riesgos hay que tener también en cuenta la modificación de la cuantía del régimen sancionador", apuntó la representante de ISMS Forum. Y es que, "aunque nosotros tenemos mucha cultura al respecto, con sanciones que pueden ir hasta los 600.000 euros, tenemos que ver cómo se aplica este cambio, que impone sanciones de hasta el 4 por ciento de la facturación del ejercicio anterior", advirtió Saracíbar. Además, se abren nuevas sanciones por desobediencia a la autoridad si no se acata su cumplimiento.

La figura del DPO

En esa línea, resultará fundamental una nueva figura que crea el Reglamento, denominada *Data Protection Officer* o DPO, necesaria en todos los organismos públicos –con la excepción de tribunales en aplicación de la función judicial– y en las entidades privadas, sean éstas consideradas responsables o encargadas del tratamiento, cuyas actividades principales conlleven "la observación habitual y sistemática de interesados a gran escala o el tratamiento a gran escala de categorías especiales de datos", según indica el texto legal.

Básicamente, se trataría de una persona o entidad independiente que, con una función claramente preventiva y proactiva, supervisa, coordina y transmite la política de protección de datos tanto en el interior de la empresa como desde dentro hacia el exterior. Para Velázquez, asesor legal de TI, se trata del "equivalente al oficial de cumplimiento". De hecho, añadió, "habrá que ver cómo conviven ambas figuras". De momento, lo que sí deja claro la normativa es que ha de ser un profesional independiente, sin conflicto de intereses y que se ocupe de las relaciones con la agencia de



Rafael Velázquez
CDPP. Consultor legal de TI

"España tiene un histórico consolidado, una forma de entender las cosas y una casuística, pero eso no quiere decir que suceda lo mismo en el resto de la UE"

Francisco Herráiz

Director de TI del Instituto Psiquiátrico José Germain

"Me parece un buen Reglamento, pero deja muchas cosas en el aire. Cuando entras en detalle, hay iniciativas importantes que no están bien definidas"

protección de datos del país correspondiente.

Se ha intentado, por tanto, dar un amplio alcance a sus funciones con el objetivo de, en palabras de Saracíbar, de ISMS Forum, "velar por el cumplimiento de las exigencias reglamentarias en el ciclo de vida del dato". Para ello, eso sí, ha de contar con una serie de conocimientos, habilidades y cualificaciones demostrables.

Además, a juzgar por las opiniones recogidas por los asistentes a la mesa redonda, esta figura no debería tener problemas de compatibilidad con otros cargos de las organizaciones. Para Velázquez, asesor legal de TI, lo que sucederá es que "tendrá que estar en colaboración con el resto de departamentos corporativos como el de Legal, de TI, de Desarrollo, de Seguridad..."; y, por supuesto, "tener un encaje en el organigrama de la organización cercano a la alta dirección", añadió. Por su parte, Saracíbar, de ISMS Forum, tampoco ve "conflicto de intereses con otras figuras de la compañía", ni siquiera con el departamento de Seguridad. Además, esta nueva legislación ha intentado blindar a esos profesionales de tal forma que "no se les pueda despedir en el ejercicio de sus funciones", aseguró la representante del ISMS Forum.

Ahora bien, no todo el mundo tiene la obligación de nombrar un DPO, lo que generó ciertas dudas a los asistentes. Por ejemplo, para Saracíbar, de ISMS Forum, "hay tres supuestos en los que es obligado este nombramiento. Uno es la Administración Pública, pero ¿qué pasa si soy concesionaria de una adjudicación?", se preguntó. La segunda es que la actividad desempeñada sea tratamiento de datos a gran escala.

Rafael García del Poyo

Presidente del Comité Asesor de Eurocloud

"El Reglamento no es ni bueno ni malo, sino, simplemente, lo que toca en estos tiempos. La dificultad radica en saber si este tipo de fórmula legal es el mejor mecanismo"

Pero, "¿qué se considera como tal, el *Business Intelligence*, el *Big Data*...?", añadió. Y la tercera se refiere a los que tengan un tratamiento especial de datos, como el sector sanitario, de

Durante la mesa redonda se tocaron distintos temas como cuál será el papel que desempeñe la LOPD con la entrada en vigor del nuevo Reglamento, o cuáles son las características más destacadas de la introducción de la figura del DPO.

telecomunicaciones, etc. "Y si no tengo que nombrar un DPO según estos tres supuestos, ¿se relajan las exigencias en cuanto a la posición de la figura que en la organización vele por el cumplimiento de esta normativa?", se volvió a cuestionar la invitada.

Geijo, de APEP, por su parte, puso sobre la mesa otro problema que aprecia en cuanto al encaje de la figura del responsable del dato dentro la empresa. "Mi duda es si convertirse en DPO no puede llegar a resultar un regalo envenenado". Y es que, teniendo en cuenta la cantidad de información que ha de controlar y procesar, así como la gestión de riesgos que debe hacer en función de ello, se corre el riesgo, según el directivo, de que este cargo se convierta en el de "una persona a la que nadie quiere contarle nada".

Herráiz, del Instituto Psiquiátrico José Germain, por su parte, explicó que en el caso de los hospitales de la Comunidad de Madrid, todos cuentan con este tipo de profesionales, por lo que es un camino que ya tienen recorrido. "Se trata de un equipo de distintos expertos que trabajan apoyando a los responsables de Seguridad, y en contacto permanente con la Agencia Española de Protección de Datos".

No ocurre lo mismo con las pymes, de las cuales el Reglamento no especifica nada, pero que, en opinión de Velázquez, asesor legal de TI, acabarán disponiendo de uno "por la vía fáctica". "Muchas empresas optarán por contar con los servicios de estos profesionales con el fin de tener una operativa eficiente y eficaz".

Aunque todos los asistentes reconocieron las ventajas de la aprobación del Reglamento en cuanto que refuerza los derechos de los ciudadanos sobre sus datos personales, hay aspectos en los que la normativa es un tanto ambigua.

Autoridades de control

Dejando a un lado todas estas cuestiones, el verdadero reto va a estar, según explicó Geijo, de APEP, en "concienciar a las empresas" de toda la labor que tienen que llevar a cabo ahora en la gestión de la protección de los datos personales.

Además, la normativa establece la existencia de una autoridad de control europea y da pie a la creación de entidades similares en los Estados miembros. En ambos casos, su función será supervisar la aplicación de las disposiciones del Reglamento y contribuir a ello en toda la UE con el fin de proteger a los ciudadanos en relación con el tratamiento de sus datos personales. Al respecto, los asistentes a la mesa redonda coincidieron en señalar que desconocen los criterios reales en los que se basará el cumplimiento de la normativa, porque su redacción provoca cierta ambigüedad en determinadas cuestiones. "Cada Estado podrá dotar a sus autoridades de control con otros poderes, además de los que el Reglamento establece. Por lo tanto, habrá que esperar a ver cómo se acaba legislando", apuntó Velázquez, asesor legal de TI. En palabras de Geijo, de APEP, "lo que quiere la norma es que la privacidad se incruste por completo en todas las organizaciones".

A tener todo en regla ayudará, según Saracíbar, "la posibilidad de conseguir certificaciones que sirvan como atenuantes ante esas autoridades de control y demuestren que las medidas estipuladas para mitigar riesgos son las adecuadas", explicó. Eso sí, esto servirá para modular la cuantía económica; en ningún caso eximirá de cualquier responsabilidad, la cual recaerá, indicó García del Poyo, de Eurocloud, en la propia empresa. "El responsable primero es la compañía, y luego vendrá una cadena detrás, en la que el encargado del tratamiento de los datos habrá de tener cierta responsabilidad", añadió.

Al final, como resumió García del Poyo, de Eurocloud, "un reglamento no debe dar márgenes de discrecionalidad". En vista de lo comentado, éste sí lo da, por lo que, a juicio del directivo, se trata de una norma "descafeinada". ■

Principio de transparencia

UNA DE LAS MODIFICACIONES INTRODUCIDAS por el Reglamento Europeo viene motivada por la aplicación del principio de transparencia, ya que se refuerza la información que se debe facilitar a los titulares de los datos, tanto en el supuesto de que éstos se recaben directamente del interesado como si se obtienen de otra fuente. En ambos casos, aparte de la información obligatoria establecida en la normativa española actual, se deberá informar también sobre la base jurídica del tratamiento, la intención de realizar transferencias internacionales o el plazo de conservación de los datos, entre otros aspectos.

En otras palabras, con esta formulación, la obligación de información se refuerza drásticamente, lo cual exigirá un esfuerzo considerable para los responsables del fichero, con el fin de adecuar sus cláusulas de información a los interesados, especialmente en materia de conservación de datos y transferencias internacionales. Y además, estos expertos deberán ser muy cautelosos en la manera en que facilitan la información, con el fin de poder acreditar con posterioridad que ha sido suministrada correctamente.