X Foro de la Privacidad: La cuenta atrás para el RGPD, a debate

El pasado jueves 8 de marzo de 2018 tuvo lugar la décima edición del Foro de la Privacidad del Data Privacy Institute (DPI), organizado por ISMS Forum Spain, en el que instituciones y expertos se reunieron para debatir sobre la aplicación del nuevo Reglamento Europeo de Protección de Datos (RGPD), que entrará en vigor el próximo 25 de mayo de 2018. "El 25 de mayo esto no acaba, esto empieza", así comenzaba Carlos A. Saiz, Vicepresidente de ISMS Forum Spain y Director de Data Privacy Institute, su discurso inaugural. "No lleguemos agotados a la maratón", añadió.

El evento contó con la presencia de profesionales y representantes de empresas e instituciones, tanto nacionales como internacionales, de la talla de Comisión Europea, el Grupo de Trabajo del Artículo 29 y la Agencia Española de Protección de Datos. La primera ponencia que daba cuerda a la jornada, a través de videoconferencia, fue la de Karolina Mojzesowicz, Deputy Head of Data Protection Unit at DG for Justice and Consumers, European Commission, en la que habló sobre el período de ajuste al reglamento y cómo se va a proceder desde Comisión Europea para implementar correctamente el RGPD.

Mojzesowicz explicó que este marco normativo lleva intrínseco un nuevo modelo de privacidad que se preocupa de velar por el derecho de los ciudadanos a la protección de su información personal. Esto, a su vez, no está reñido con la competitividad de las compañías. Por otra parte, ha querido recordar a las empresas que su deber es preocuparse de gestionar y controlar continuamente el flujo de los datos con las auditorías pertinentes y, sobretodo, comprobar que las empresas terceras con las que se trabaje, y que hayan manejado datos sensibles, hayan cumplido con lo expuesto en el reglamento.

RGPD: el gran reto de las empresas

La primera mesa redonda que tuvo lugar, 'GDPR: A New Data Processing Framework', contó con la participación de Rubén Cabezas, Data Protection Officer de Banco Santander; María de la Torre, Data Protection Officer de Masmovil; Henry Velásquez, European Data Protection Officer & Compliance Manager de Cigna; Ignasi Riera, Territory Account Executive Spain & Portugal de OneTrust; Juan Navarro, Responsable de Enterprise Security Products Iberia de Microfocus; Maica Aguilar, Information Security Manager de Ferrovial y miembro del Data Privacy Institute; y Álvaro Écija, miembro de ISMS Forum y fundador de ciberderecho.com, como moderador de la mesa.

Una cuestión crucial que se abordó giró en torno a los problemas que las empresas se están encontrando durante el proceso de adaptación al reglamento, teniendo en cuenta que las representadas en la mesa cuentan con una considerable cartera de clientes. "El gran desafío en este momento son los desarrollos tecnológicos, sobre todo la parte de gestión de consentimientos", respondía Rubén Cabezas. "Entramos todos en pánico, por lo que la cultura RGPD afecta al comportamiento del día a día. Lo estamos afrontando sin prisa pero sin pausa", afirmaba María de la Torre.

El Data Protection Officer de Santander comentó que existe confusión en torno a qué se puede o no hacer en base al consentimiento del cliente. Para el banco, la vía del interés legítimo es factible. No obstante, en los supuestos en los que no se cuente con esta vía, "el cliente deber ser soberano" y, sin duda, aquellas personas que den su sí para el envío de una acción comercial constituyen un público objetivo más interesado. Con este aspecto coincide también la DPO de Masmovil, "el target de clientes que finalmente digan sí o no será un target real. No como ahora, que nos encontramos ante una base de síes o noes indeterminada".

Determinar cómo se gestionan los consentimientos es una tarea prioritaria para las compañías en el marco normativo del RGPD. "Hemos apostado por aplicar mejores prácticas e incluso en las jurisdicciones donde no necesitamos el consentimiento, requerimos que nuestros clientes o beneficiarios del seguro, cuando accedan al portal web, reconozcan electrónicamente que han entendido el flujo de los datos que se proponen en la cláusula de información", explicaba Henry Velásquez.

Hacer mayor de edad a la privacidad

El Reglamento Europeo de Protección de Datos introduce un enfoque diferente al concepto del dato. En palabras de María de la Torre, "el cambio más importante es que el dato ya no forma parte de un activo de la compañía, sino que es propiedad del cliente". No obstante, esto no tiene por qué ser negativo para la competitividad del mercado. La idea general de la mesa redonda se centró más bien en entender este nuevo reglamento como una oportunidad de negocio para las empresas, y no tanto como una obligación estrictamente normativa.

De igual manera, hablamos de un proceso que requiere de varias fases. "Algunas empresas ya han realizado avances orientados a servicios y los proveedores de tecnología ya han adaptado sus mensajes a la GDPR".

Eso sí, "algunos han subido al tren con expectativas y no tienen claro si el tren es un AVE o un cercanías", comentaba Juan Navarro.

Según Maica Aguilar, el mundo de la privacidad en España ha estado "muy encorsetado" por la LOPD y que, por lo tanto, con el nuevo reglamento tenemos la ocasión de "desabrochar ese corsé y empezar a pensar las cosas". Para la representante de Ferrovial, existen muchos paralelismos entre la seguridad, los modelos de gestión y de organización, y los análisis de riesgos que ya se están aplicando, con lo que está pidiendo el reglamento. "El RGPD es una oportunidad para hacer mayor de edad a la privacidad", afirmaba Aguilar.

¿Cómo crear una cultura de la privacidad?

Una de las conclusiones que se pueden extraer de las disposiciones del Reglamento Europeo de Protección de Datos es que debemos empezar a caminar hacia una cultura de la privacidad global. Pero, ¿cómo desarrollarla? ¿Existen claves para hacerla realidad? Henry Velásquez lo tiene claro: "La apuesta debe ser la comunicación y sinergias entre los diferentes departamentos. El riesgo derivado de un incumplimiento normativo puede convertirse en un riesgo operacional, y como te quiten la licencia en determinados territorios, ya no haces negocio. Es un tema que va más allá de cumplir con el reglamento porque me lo exigen, porque el mercado y los clientes te lo exigen también".

Por su parte, según Ignasi Riera, a las personas les gusta que la privacidad "esté cerca de ellos" y que cumpla con la normativa establecida. En palabras del representante de OneTrust, el enfoque de la compañía se ha fundamentado en "dejar la seguridad a un lado y dedicarnos a privacidad. Es verdad que no existe privacidad sin seguridad pero, cuando hablamos de seguridad, nos referimos a infraestructuras y, cuando hablamos de privacidad, hablamos de proteger al individuo".

La figura del Data Protection Officer (DPO)

Durante la mesa redonda también se debatió sobre cómo se debe entender la figura del Data Protection Officer (DPO) bajo este nuevo reglamento. "De entre todas las funciones del DPO, la que es clave, es la de persuadir a la empresa para que todas las decisiones que adopten y que impliquen un tratamiento de datos de carácter personal, tengan en cuenta las obligaciones derivadas del RGPD, y eso es una labor de transversalidad, de estar en el día a día de los diferentes comités y proyectos", explicaba Cabezas.

Asimismo, el DPO de Santander añadió con especial hincapié que donde más debe estar presente esta figura es en el área de formación. "No podemos basarnos en un curso de e-learning con diez preguntas que se hagan una vez al año, sino que debe ser esa labor de extender todas las obligaciones de RGPD a cada uno de los departamentos. Queda esa fase de privacy by design, de realmente integrar el reglamento en todos los productos, no como un mero compliance, sino como un valor añadido".

Ir más allá del cumplimiento normativo

La jornada continuó con la participación de Isabel Tristán, Security Client Executive at Cognitive Solutions Unit, IBM, a través de una conferencia basada en la idea de no quedarse única y exclusivamente con lo expreso en el reglamento y tratar de ser cada vez seguros en el manejo de los datos, ya que ahora no solo se encuentran en entornos tradicionales, sino también en Cloud.

En este sentido, el cifrado adecuado de los datos se hace obligatorio. "Si perdemos las llaves de encriptación y cifrado, podemos perder los datos. Es importante separar los roles entre quién gestiona las llaves y quién gestiona los datos", comentaba Tristán. Al parecer, no sólo se trata de cifrar, sino de administrar adecuadamente las llaves de cifrado, y eso conlleva utilizar un estándar de mercado con el que poder gobernar de forma centralizada, proporcionar auditoría de su uso, que la persona que gestiona las llaves no sea la misma que gestiona los datos, y revisar el ciclo de vida de las llaves.

El decálogo de la notificación de brechas

Giuseppe D'Acquisto, Technology Adviser, Italian Data Protection Authority y miembro del Article 29 Working Party, dio diez claves para gestionar adecuadamente una brecha de datos, si se da el caso.

1. Sea precavido al etiquetar un incidente de seguridad como una violación de datos personales.

2. En la notificación de violación de datos, el riesgo es mayor.

3. La gobernanza y la asignación de responsabilidades son muy importantes.

4. La notificación de brechas de datos y las reglas de comunicación aplican también a los controladores no basados en la UE.

5. Primero espera a que transcurra el umbral de 72 horas para la notificación de la brecha y, posteriormente, hacer más investigaciones.

6. Ser procesadores no reduce responsabilidades de notificación de violación de datos.

7. Cuando hay un alto riesgo, el tiempo de comunicación se desarrolla más rápido.

8. No deje solos a los sujetos de datos con la solución de los incidentes.

9. Ser proactivo en la mitigación de las consecuencias de una violación puede ser una estrategia gratificante.

10. Aprende de tus propios errores (si hay alguno).

No habrá moratoria a partir del 25 de mayo

Mar España, directora de la Agencia Española de Protección de Datos (AEPD), aclaró durante su intervención en el Foro de la Privacidad que el Reglamento Europeo de Protección de Datos será de obligado cumplimiento a nivel europeo para grandes compañías, pymes, autónomos, y administraciones públicas. "No va a haber moratoria a partir del 25 de mayo. Ese día tantos las administraciones públicas como las empresas privadas tienen que estar en disposición con las obligaciones del nuevo reglamento".

Para Carlos A. Sáiz, "es lógica la postura de la AEPD de no conceder ninguna moratoria. La norma se aprobó en el 2016, con un plazo de dos años. Es una obligación legal para las empresas cumplirla y para la Agencia controlar su aplicación". A su vez, convendría tramitar un proyecto de ley en el congreso que pudiera entrar en vigor al mismo tiempo que el RGPD, ya que introduce nuevas normas que hay que saber interpretar a nivel interno. De lo contrario, "la norma nacional se quedaría coja ante el nuevo panorama", señala España.

El foro también fue escenario de presentación de las Guías de Análisis de Riesgos y Evaluación de Impacto en la Protección de Datos Personales, de la mano de Mar España y Andrés Calvo, responsable de la Unidad de Evaluación y Estudios Tecnológicos de la AEPD.

La primera de ellas recoge una metodología adecuada para evaluar el nivel de riesgo en relación con los tratamientos de datos personales que realizan las organizaciones. Por su parte, la segunda, permite a las organizaciones identificar los riesgos que un sistema, producto o servicio puede implicar para los derechos y libertades de las personas y, tras haber realizado ese análisis, afrontar y gestionar esos peligros antes de que se materialicen.

La resiliencia: imprescindible para afrontar las amenazas

La segunda mesa redonda que tuvo lugar, "Resilience as Data Protection Defender", contó con la participación de Phil McQuitty, Senior Director, Identity and Data Governance Strategist, Sailpoint; Raúl Pérez, Global Security Solutions Architect, Panda Security; Alfonso Hermosillo, Senior Sales Engineer EMEA, Securonix; Vincent Vanbiervliet, Product Manager Data Protection, Sophos; Luca Nilo Livrieri, Manager Sales Engineering, Forcepoint Italy & Iberia; y Roberto Baratta, Global Executive VP and Director of Loss Prevention, Business Continuity and Security, Abanca, y miembro de ISMS Forum.

La resiliencia es un término esencial dentro del mundo de la protección de datos. Es necesario invertir un gran empeño en la visibilidad, control y capacidad de reacción cuando hablamos de un ciberataque. Durante la charla, los ponentes apuntaron que esto se hace imprescindible porque con la entrada del Reglamento es obligatorio notificar las infracciones.

Podemos visualizar tres áreas principales en este proceso. La primera la constituye las medidas preventivas, que suponen controlar los accesos y los permisos de las personas. La segunda, las medidas de detección, es decir, vigilar la actividad y comprobar si las copias de seguridad se están ejecutando. Y la tercera y última: la capacidad forense. Esto quiere decir, por ejemplo, que ante una consulta del usuario sobre cuándo se accedió a sus datos y quién lo hizo, éste debe obtener respuesta.

Asimismo, la mesa planteó la necesidad de desarrollar protocolos de colaboración entre los diferentes departamentos. Esto se traduce, por ejemplo, en que las soluciones de malware colaboren con la identidad de gobierno para notificar que la cuenta de usuario de una persona ha sido comprometida, de manera que posteriormente una interfaz envíe una solicitud de acceso. Estas colaboraciones podrían ser muy útiles incluso para predecir futuras amenazas.

Defender los derechos humanos: una misión complicada

El punto y final del programa de ponencias lo dio Paul de Hert, International fundamental rights expert, quien se mostró como "un gran fan" de la europeización de los derechos humanos, con una visión positiva respecto al panorama que el reglamento plantea. "Va a ser difícil defender los derechos fundamentales, pero la Unión Europea está en ello, al menos algunos actores y al menos en algunos asuntos".

No obstante, también expresó sus dudas a través de interrogantes que deben preocupar en materia de derechos humanos. Uno de ellos es que, según su visión, el enfoque europeo respecto a la protección de los datos no garantiza algunas líneas democráticas. En este sentido, el ponente ve dos problemas: la delegación política y la seguridad jurídica.

Otro de los aspectos importantes que aún deben ser resueltos es la "relación entre la directiva y las normas de derecho público de la Unión Europea sobre la protección de los datos personales". El Supervisor Europeo de Protección de Datos (SEPD) es particularmente crítico con la propuesta de tratar los datos personales como un objeto de contragarantía contractual, ya que considera que los datos deben verse exclusivamente desde la perspectiva de los derechos fundamentales y, por lo tanto, no pueden monetizarse.

El X Foro de la Privacidad contó con la presencia de más de 350 asistentes. Un año más, se constituyó como un encuentro entre profesionales, empresas e instituciones expertas en protección de datos, con el fin de debatir sobre el presente y futuro del sector y la aplicabilidad del Reglamento General de Protección de Datos, que entrará en vigor el próximo 25 de mayo y que, sin lugar a dudas, marcará un antes y un después en el ámbito de la ciberseguridad y la privacidad, haciendo especial énfasis en la notificación de brechas de seguridad.