**El foro de expertos DENAE-Queen Mary University analiza la economía de datos europea ante el reto del Brexit**

La Secretaría de Avance Digital acogió el pasado 29 de octubre el foro DENAE-Queen Mary University sobre los riesgos y oportunidades que plantea la aplicación del Reglamento General Europeo de Protección de Datos (RGPD) para la economía de datos europea en el contexto cambiante del Brexit.

En su presentación del foro, Cristina Morales, de la Secretaría de Estado de Avance Digital y Mabel Klimt, Presidenta de DENAE, destacaron la importancia de celebrar esta clase de eventos con autoridades, académicos y expertos en protección de datos y ciberseguridad, del Reino Unido y de España, especialmente, en este contexto de incertidumbre generalizada ante el Brexit.

**El RGPD «no va sólo de multas»**

En la primera mesa, moderada por la profesora de la Universidad Rey Juan Carlos, Estrella Gutiérrez, el panel de expertos discutió sobre los retos que plantea el cumplimiento de las obligaciones establecidas en el RGDP.

Ian Walden, director del Centro de Estudios de Derecho Mercantil de la Queen Mary, y miembro del Grupo de Expertos en protección de datos de la Comisión Europea, advirtió que «el RGPD no va sólo de multas», sino que existen otros instrumentos correctivos como las recomendaciones, amonestaciones, requerimientos de información o de adopción de medidas correctoras que garantizan el cumplimiento normativo.

Por su parte, el responsable internacional de la AEPD, Rafael García Gonzalo puso en valor la actividad regulatoria y preventiva de la Agencia frente a la meramente sancionadora, ante las dificultades que plantea la determinación de las sanciones a aplicar. «No podemos cambiar de forma drástica» desde el sistema anterior de la Directiva al nuevo régimen de sanciones administrativas que prevé el RGPD. Los criterios modificativos de la responsabilidad por incumplimiento del Reglamento Europeo necesitan de una «aplicación coherente a lo largo de toda Unión Europea».

Silvia Ruiz, de Écija Abogados y DPO de una Agencia de Medios con sede en el Reino Unido, subrayó los retos a los que se enfrentaba en su rol de Delegada de Protección de Datos para asegurar el cumplimiento del Reglamento dada la continua evolución tecnológica y las nuevas necesidades del negocio.

**Mitigando los riesgos del Brexit**

El segundo panel, moderado por Ian Walden, giró en torno a riesgos del Brexit en el contexto de la economía de datos europea. Por su parte, Raúl Rubio, de Baker & McKenzie, puso de manifiesto el incremento de coste para las empresas que provocará Brexit debido a la duplicidad de obligaciones, procedimientos y registros de tratamientos. Sin embargo, Raúl Rubio advirtió de la complejidad a la que habrán de enfrentarse las empresas a la hora de gestionar las transferencias internacionales de datos que tengan su origen en España, pasen por el Reino Unido y tengan como destino final EE.UU.

Paula Ortiz, de IAB España, centró su exposición en la regulación sobre «e-Privacy» y adelantó que ya se están adoptando soluciones preventivas para la protección de datos en el sector de la publicidad, el marketing y la publicidad digital. «El GDPR y el e-Privacy parten del mismo enfoque», y ambos grupos normativos son aplicables al tratamiento de datos personales de usuarios europeos.

Finalmente, Ulrich Wuermeling, profesor de la Universidad Queen Mary y abogado experto en privacidad de la firma internacional, Latham & Watkins, cerró este panel analizando los inconvenientes que podrían plantear los diferentes instrumentos existentes para llevar a cabo transferencias internacionales de datos aplicables tras el Brexit. Así, por ejemplo, en el caso de las «normas corporativas vinculantes» (BCRs), el experto subrayó que se trata de un procedimiento largo, donde no siempre queda claro quién es la Autoridad de control competente. A su vez, «el consentimiento explícito −advirtió Wuermeling− no es una opción fácil» en la que puedan apoyarse tales transferencias.

**Consideraciones prácticas: «Sé tan rápido como tu ecosistema»**

La última de las mesas del evento, moderada por Pilar Cousido, de la Universidad Complutense de Madrid, abordó cuestiones y recomendaciones prácticas en materia de cumplimiento normativo en protección de datos y prevención frente a incidentes.

La abogada experta en ICT e investigadora de la Universidad Queen Mary, Laura Aliaga, abundó en la importancia de diferenciar claramente entre responsables, encargados y corresponsables de tratamiento, especialmente, a raíz de la última jurisprudencia europea (Facebook Fan Page y Fashion ID), donde el Tribunal de Luxemburgo ha calificado de corresponsables de tratamiento a Facebook y a las empresas que insertan el plug-in «Me gusta» en su página web o al administrador de una página de fans en la red social.

La confusión entre el responsable, el encargado y los corresponsables de tratamiento no es algo que las organizaciones puedan tomarse a la ligera, pues a juicio de Laura Aliaga, ello puede tener consecuencias negativas graves para las partes involucradas, entre otras, el incumplimiento de las obligaciones del responsable, la nulidad de las cláusulas contractuales que regulen la relación entre responsable-encargado; las eventuales reclamaciones e indemnizaciones y, en última instancia, el riesgo reputacional de las organizaciones que hayan identificado erróneamente sus encargos o tratamientos conjuntos.

Christopher Millard, co-director del Centro de Investigación de Cloud Computing de Microsoft y también profesor de la Universidad Queen Mary, analizó desde el punto de vista práctico el cumplimiento del RGPD entendido como un «servicio al cliente». Para Millard, el RGPD ha creado una mutua interdependencia «tan compleja» entre responsables y encargados, que el cumplimiento de la norma se antoja una tarea «abrumadora y compleja», en especial para las PYMES. En un futuro próximo en el que habrá «más de un trillón de dispositivos conectados a través de Internet de las cosas», el experto abordó, a través de distintos estudios de caso, cómo la prestación de servicios en nube incluye no solo compromisos u obligaciones por parte del prestador de cumplir el RGPD sino que, además, las cláusulas contractuales incluyen ya servicios específicos a los clientes de cumplimiento normativo.

Finalmente, Alfredo Reino, experto en ciberseguridad de Secureworks, destacó que, si bien los datos personales quedan expuestos en los ciberataques, el principal objetivo de estos delitos «no es en su inmensa mayoría de casos el robo de datos sino de dinero». Por ello y dado que la prevención total de estos ataques es imposible, recomendó concentrar esfuerzos en la detección temprana y en dar una respuesta rápida y coordinada cuando sucedan. Cómo recomendación práctica a seguir para las organizaciones: «Sé tan rápido como tu ecosistema», e implementa planes específicos de respuestas a incidentes.