FUNDACIÓN ESYS Empresa Seguridad Y Sociedad

Una revisión de la agenda digital europea en 2022

Cuaderno ESYS | Raquel Jorge Ricart – noviembre 2022

Introducción

Con la vuelta de septiembre, el escenario de la agenda tecnológica tanto europea como española para el tiempo restante de 2022 se muestra activo. Algunos temas buscan ser finalizados antes del nuevo año; otros temas se encuentran en el ecuador de las negociaciones y discusiones; y varios asuntos acaban de ser propuestos para enmarcar el programa de lo que ya será 2023.

Finalizar, acelerar y abrir nuevos temas en materia digital para el año 2023 es estratégico, puesto que terminan los mandatos políticos. 2023 será el último año al completo de doce meses para el mandato del Colegio de Comisarios de la Comisión Europea, que será renovado en 2024. También lo es para España, ya que la fecha actualmente prevista para las elecciones generales es en noviembre de 2023.

Temas de mayor carácter estratégico en 2022

Además de la negociación sobre los detalles del Reglamento Europeo de Inteligencia Artificial, que son de largo recorrido, en 2022 ha habido otros temas candentes, como los siguientes.

1) Propuesta de Reglamento Europeo de Datos (Data Act)

En febrero de 2022, la Comisión Europea presentó la propuesta de Reglamento Europeo de Datos. La propuesta nació de la Comunicación sobre una estrategia europea para los datos, adoptada por la Comisión Europea en febrero de 2020, que destacaba la necesidad de fomentar el intercambio de datos entre empresas y gobiernos en aras del interés público, apoyar el intercambio de datos entre empresas y evaluar el marco de los derechos de propiedad intelectual con vistas a seguir mejorando el acceso y el uso de los datos.

Los objetivos del Reglamento Europeo de Datos son contribuir a medidas que permitan a los usuarios de dispositivos conectados acceder a los datos generados por ellos y compartir dichos datos con tercero; evitar abuso en contratos de intercambio de datos; regular el uso de datos en poder del sector privado por parte del sector privado, que sean necesarios para circunstancias excepcionales, especialmente en caso de emergencia pública, como inundaciones e incendios forestales, o para aplicar un mandato legal si los datos no están disponibles de otra manera.

Actualmente la propuesta se encuentra en un estado de debate. En el Parlamento Europeo, la comisión responsable es la Comisión de Industria, Investigación y Energía (ITRE), a cargo de la eurodiputada española Pilar Del Castillo Vera (PP) como ponente.

Varias implicaciones de la propuesta de Reglamento Europeo de Datos podrían ser:

- Su **interrelación con propuestas regulativas paralelas, como es el Reglamento de Gobernanza de Datos** (Data Governance Act), que regula el uso, acceso y compartición de datos procedentes del sector público así como qué significa ser una “organización altruista de datos”.
- Las **posibilidades de competitividad económica e industrial para los Espacios Europeos de Datos (Data Gateway)** que se están creando desde un punto de vista sectorial para diez ámbitos estratégicos: salud, agricultura, fabricación, energía, movilidad, finanzas, administración pública, competencias, la Nube Europea de Ciencia Abierta, y la prioridad transversal clave de cumplir los objetivos del Pacto Verde.

- Las oportunidades que el Reglamento Europeo de Datos puede brindar para el **posicionamiento global de la UE a través de la convergencia regulatoria con terceros países en sus crecientes diálogos bilaterales**, como es el caso del Consejo de Comercio y Tecnología UE-EEUU (TTC), el TTC con India, o los "Digital Partnership Agreements" con Corea del Sur, Japón y Singapur.

2) Propuesta de Ley Europea de Chips

La propuesta de Ley Europea de Chips fue presentada en febrero de 2022 por la Comisión Europea. El objetivo es el de mejorar el ecosistema de semiconductores en Europa. Se estructura en tres pilares:

- Impulsar la creación de capacidades tecnológicas a gran escala y la innovación en el ecosistema de chips de la UE. Se espera que la iniciativa mejore la transición "del laboratorio a la fábrica".
- Mejorar la seguridad de suministro de chips, mediante la atracción de nuevas inversiones, la creación de espacios de producción integrada, y la creación de proyectos pilotos en Estados miembro, entre otros;
- Desarrollar un mecanismo de monitoreo y respuesta a crisis. La Comisión debe llevar a cabo una "evaluación de riesgos de la Unión" sobre los riesgos para el suministro de semiconductores en la UE, que debe identificar un conjunto de indicadores de alerta temprana.

Ha emergido un debate relevante en torno a la propuesta: **la posibilidad de aplicar subsidios** para apoyar la creación y crecimiento de fábricas de semiconductores. El objetivo de la Comisión es ofrecer subsidios para aquellos proyectos que demuestren necesitar dichas ayudas, que el efecto resultante de ese subsidio sea un impacto paneuropeo positivo, y que sea proporcional. Algunas visiones están en contra de estos subsidios por los requerimientos administrativos que puede suponer, mientras otras perspectivas consideran que la Unión Europea está siguiendo el modelo de subsidios en chips que otros países ya están realizando.

Un aspecto estratégico será el **"Joint Undertaking" (JU)** que acompañará a la Ley Europea de Chips. El JU será la plataforma por la que se materializarán en la práctica los proyectos industriales bajo los tres pilares.

3) Reglamento Europeo de Resiliencia Cibernética (Cyber Resilience Act)

El 15 de septiembre de 2022, la Comisión Europea hizo pública su propuesta de Reglamento para mejorar la ciberresiliencia de la ciudadanía europea.

Actualmente los productos de hardware y software que adquirimos pueden estar sujetos a vulnerabilidades. Según la UE, los costes de las brechas de seguridad de los datos ascienden a 10.000 millones de euros al año. Y lo que aún es peor: los usuarios desconocen estas vulnerabilidades habitualmente.

La propuesta de Reglamento busca reducir las vulnerabilidades mediante la definición clara del reparto de responsabilidades de fabricantes de hardware y desarrolladores de software, no solamente en el diseño, sino a lo largo de toda la vida del producto.

Por otro lado, la mejora de la transparencia en cuanto a las características y garantías del producto permitirá que los usuarios realicen compras de una manera informada y estén protegidos por la garantía del fabricante ante posibles vulnerabilidades.

Existen varios aspectos clave en torno al Reglamento de Ciberresiliencia (Cyber Resilience Act):

- El anexo adjunto a la legislación establece que **habrá dos categorías de productos**: una para los productos críticos, que cubrirá alrededor del 10% del mercado, y una segunda categoría que abarcará el resto ed productos.

  Para los productos de bajo riesgo, la Comisión pedirá a las empresas que realicen una autoevaluación, indicando que un producto cumple con las normas de ciberseguridad. Para los que puedan presentar un riesgo significativo de ciberseguridad, el fabricante tendrá que demostrar que cumple los requisitos ante una autoridad nacional o mediante una evaluación de terceros.

- La Comisión Europea **plantea tener la facultad de ordenar a la Agencia de Ciberseguridad de la UE, ENISA**, que evalúe si un producto presenta un "riesgo significativo para la ciberseguridad" y lo retire del mercado en caso de que así sea.

El nuevo proyecto de Reglamento aún debe ser revisado por el Parlamento Europeo y el Consejo de la UE, lo que permitirá lanzar los trílogos, antes de convertirse en reglamento en caso de aprobarse.

4) Reglamento Europeo de Libertad de los Medios de Comunicación (European Media Freedom Act)

La Comisión Europea presentó su propuesta de Reglamento y la Recomendación relativa al Reglamento Europeo de Libertad de los Medios de Comunicación (Media Freedom Act).

La propuesta de Reglamento incluye salvaguardias contra la injerencia política en las decisiones editoriales y contra la vigilancia. Hace hincapié en la independencia y la financiación estable de los medios de comunicación de servicio público, así como en la transparencia de la propiedad de los medios y de la asignación de la publicidad estatal.

También establece medidas para proteger la independencia de los editores y revelar los conflictos de intereses. Por último, la propuesta de Reglamento abordará la cuestión de las concentraciones de medios de comunicación y creará un nuevo Consejo Europeo de Servicios de Medios de Comunicación independiente, integrado por las autoridades nacionales de medios de comunicación. La Comisión también ha adoptado una Recomendación complementaria para fomentar las salvaguardias internas de la independencia editorial.

Temporalmente, la propuesta de la Comisión Europea se lanzó el 16 de septiembre de 2022. El nuevo proyecto de Reglamento aún debe ser revisado por el Parlamento Europeo y el Consejo de la UE, lo que permitirá lanzar los trílogos, antes de convertirse en reglamento en caso de aprobarse.

5) Reglamento DORA

La propuesta de Reglamento de Resiliencia Operativa Digital, “DORA” por sus siglas en inglés, tiene una **relevancia y carácter crítico** por su objetivo de mejorar la resiliencia y capacidad de respuesta de entidades financieras frente ataques cibernéticos e incidentes de las TICs.

Algunos de los aspectos principales de este acuerdo es que DORA busca regular el sistema de notificación de incidentes TIC mediante la siguiente vía: las empresas deben informar a sus usuarios y clientes cuando el incidente tenga o pueda tener un impacto en sus intereses financieros y ahora tendrán también el requisito de notificar a las autoridades competentes aquellas interrupciones TIC graves. Además, en el texto se garantiza que dentro de los próximos dos años se establecerá una única plataforma a nivel europeo para notificar incidentes graves del servicio de Tecnologías de la Información (IT).

Es una regulación, no solo estratégica, sino también crítica, para la seguridad, competitividad económica y garantía de los derechos fundamentales de la Unión Europea. Hasta ahora, no ha habido una efectiva coordinación en todo el ciclo de gestión de la ciberseguridad para las entidades financieras ubicadas a lo largo de la Unión Europea: ni en la forma en que se abordaba el ciclo (identificación, protección, prevención, respuesta y recuperación) ni en una comunicación ni cohesión de las políticas públicas y gestión de crisis entre sectores y entre Estados miembros.

La reglamentación aplicará a entidades financiera reguladas a nivel europeo tales como bancos, intermediarios de seguros, firmas de inversión, entidades de dinero electrónico, proveedores de servicios IT, proveedores de nube, auditores legales, sociedades de gestión, agencias de calificación, entre otros.

En ese sentido, **varios retos -y, por tanto, oportunidades- se presentan para la efectiva implementación, ejecución y gestión de la propuesta de reglamento DORA**:

- Capacitar a las entidades financieras de adecuados canales de comunicación para la notificación de incidentes;

- Fomentar una "cultura de ciberseguridad" realmente integral, que conciba DORA no solo como una regulación que cumplir al uso, sino también una forma de transformar las organizaciones en su conjunto para ser resilientes en el largo plazo, de manera eficiente y que permee desde las altas direcciones de las empresas hasta los puestos más tácticos dentro de la organización.

- Establecer una publicación periódica -anual o cada dos años- donde se reporten los aprendizajes y lecciones más importantes de la implementación de DORA en sí, y de las enseñanzas, mejoras y retos que han experimentado las entidades del sector financiero tras hacer uso de ella.

Todo ello permitirá mejorar la regulación así como la propia vida de las empresas en un mundo cada vez más digitalizado. Estas medidas son un pilar fundamental que ayudará a la UE y a sus actores a ser más resilientes y seguir apoyando el bienestar económico y social de la región.

6) Directiva NIS 2.0

La revisión de la Directiva NIS, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, supone una actualización estratégica de aspectos que, si bien ya mejoraron las capacidades de los Estados miembros para dar respuesta a las ciberamenazas, cibervulnerabilidades y ciberataques con la Directiva original, ahora supone una mejora en lo que se refiere a la gobernanza, gestión, *reporting* y respuesta coordinada ante estos riesgos de seguridad.

Algunas de las **mejoras que se solicitaron realizar**, en varios informes del Parlamento Europeo, consistían en:

- Endurecer las obligaciones de ciberseguridad en cuanto a la gestión de riesgos, las obligaciones de información y el intercambio de información.
- Reducir la carga administrativa y mejorar la notificación de incidentes de ciberseguridad.
- Necesidad de que los Estados miembros cumplieran con medidas de supervisión y ejecución más estrictas, y armonizar sus regímenes de sanciones.
- Ampliar el ámbito de aplicación sectorial para incluir también a las instituciones académicas, de conocimiento e investigación, que la Comisión había dejado fuera del ámbito de aplicación de su propuesta de la NIS2, mientras que muchas estrategias nacionales de ciberseguridad las cubren.
- Simplificar las obligaciones de notificación de incidentes para evitar un exceso de información;

Otro aspecto relevante es que NIS2 ha introducido criterios adicionales para determinar las entidades que deben estar cubiertas por la Directiva, **excluyendo del ámbito de aplicación a las entidades que operan en el ámbito de la defensa o la seguridad nacional, la seguridad pública, las fuerzas de seguridad y el poder judicial, así como los parlamentos y los bancos centrales**.

Asimismo, la **coherencia jurídica** de la Directiva le ha permitido alinearse con otras propuestas como son la Directiva sobre la resiliencia de las entidades críticas (Directiva CER) y la propuesta de Reglamento sobre la resiliencia operativa digital para el sector financiero (DORA).

Nuevas medidas anunciadas en el Discurso sobre el Estado de la Unión (SOTEU 2022)

Si bien estuvo marcadamente centrado en la situación en Ucrania, lo que dio al discurso un carácter geopolítico, político, poco habitual de anteriores SOTEU, que habían sido tecnocráticos en general, la Presidenta de la Comisión Europea anunció varias medidas alineadas con el paquete digital:

- **Propuesta de Ley de Materias Primas Críticas**

Este aspecto es particularmente relevante para la Unión Europea y sus Estados miembros, dado que las materias primas críticas generan un alto grado de dependencia en terceros países y posibles vulnerabilidades ante la llegada de suministros y posibles shocks de comercio internacional.

En particular, las materias primas críticas son esenciales para la tecnología avanzada, para apoyar las fases del proceso industrial -tanto para productos tecnológicos como no tecnológicos- y, en particular, para tecnologías verdes como las turbinas eólicas, los vehículos eléctricos, la iluminación de bajo consumo o los paneles solares.

El Estudio de Prospectiva de la UE de 2020, llamado "Materias primas críticas para tecnologías y sectores estratégicos en la UE", muestra las necesidades, capacidades y dependencias de cada una de las materias para un número importante de productos y tecnologías en el seno de la UE. La procedencia de estas materias primas críticas de terceros países añade una capa mayor de vulnerabilidad.

Algunas de las implicaciones de esta propuesta son:

- La necesidad de que haya un **desarrollo temprano** de esta propuesta de ley.
- La **complementariedad de este expediente legislativo con una estrategia mayor de política industrial** que promueva la coordinación entre sectores, administraciones públicas y empresas del sector privado entre los Estados miembros, y que suponga una aceleración y una gobernanza común de las distintas estrategias que ya se han lanzado hasta ahora, como son la Alianza Industrial de Materias Primas, la Comunicación sobre Materias Primas Críticas de 2020 o la metodología de identificación de materias primas críticas.
- El fortalecimiento de un **mecanismo de alerta temprana** ante posibles shocks en la cadena de suministros.
- El **aprovechamiento de materias primas que se encuentran en suelo europeo** y que no han sido explotados.

- **Iniciativa sobre mundos virtuales, como el metaverso**

Si bien no ha habido mayores desarrollos todavía en esta materia, ya a principios de 2022 la Comisaria de Competencia, Margrethe Vestager, declaró que el metaverso sería otro aspecto a considerar para una posible futura regulación. La razón proviene de la actual tendencia a la compra y adquisición de pequeñas empresas con alta capitalización y especialización de productos por parte de grandes empresas.

- **Propuesta para el Año Europeo de las Habilidades**

Se espera que vaya alineado con las medidas ya orientadas de la Brújula Digital 2030.

Conclusiones

La gran parte de medidas más sonadas fue anunciada en 2020, con el contexto de la pandemia producida por la Covid-19, que había acelerado la digitalización en pocos meses y ante cuyos efectos no se había dado respuesta. Ello explica que en 2020 se anunciaran las propuestas de Reglamento de Servicios Digitales (DSA) y de Mercados Digitales (DMA), que se han encauzado a una velocidad ingente. Posteriormente, otras iniciativas fueron la revisión de la Directiva NIS 2.0 y las medidas reseñadas anteriormente, así como las negociaciones sobre el Reglamento de Inteligencia Artificial o las iniciativas del "derecho a la desconexión digital".

En ese sentido, 2022 es un año de "madurez" o de "asentamiento" de la agenda tecnológica y digital: de lo que ya se anunció y se está madurando durante estos doce meses, y de aquellas iniciativas últimas a lanzar durante el año 2023 para ser cerradas o anunciadas antes de las siguientes elecciones en 2024, dado que el mandato del Colegio de Comisarios podría cambiar. La agenda tecnológica y digital de la Unión Europea en 2022 se presenta activa.