Año nuevo, nuevo "paquete" de ciberseguridad de la Comisión para 2021

Félix Arteaga | Investigador principal, Real Instituto Elcano.

La Comisión Europea cerró 2020 con un paquete de medidas destinadas a adaptar la ciberseguridad europea a la transformación producida por el proceso de digitalización de los últimos años acelerado por el COVID-19. *CIBER elcano* y el Grupo de Trabajo de Ciberpolítica del Real Instituto Elcano irán analizando su impacto en España a lo largo de los próximos meses, pero, en conjunto, el paquete refleja la creciente europeización de la ciberseguridad en la UE para apoyar la transformación digital.

La Comisión Europea amplía y profundiza su influencia en todos los aspectos de la ciberseguridad mediante sus agendas para 2020 y para los años posteriores a 2021, que se resumen en el cuadro siguiente:

Agenda 2020

- Estrategia para la Unión de Seguridad 2020-2025
- Inclusión de la ciberseguridad en los fondos Repair and Prepare for the Next Generation
- Estrategia de Ciberseguridad de la UE para la Década Digital
- Propuesta para la actualización de la Directiva NIS
- Propuesta para una Directiva sobre la resiliencia de entidades críticas

Agenda 2021 y siguientes

- Implementación de medidas relativas a la ciberseguridad de redes 5G (EU Toolkit Box)
- Creación de la Joint Cyber Unit para la coordinación operativa de los Estados miembros
- Definición de esquemas de certificación EU Cybersecurity Act
- Regular el acceso a comunicaciones cifradas para compatibilizar la privacidad y la interceptación legal de comunicaciones
- Revisión de Directiva ePrivacy, sobre privacidad y confidencialidad de las comunicaciones electrónicas
- Inversiones 2021-2027: Digital Europe Programme, Horizon Europe y Recovery Plan for Europe

La agenda saliente

Las agendas aspiran a consolidar una transformación digital cibersegura en la UE. En febrero de 2020, la Comisión reivindicó que el futuro de la UE pasaba por configurar su futuro digital, para lo que a lo largo del año se han ido dando pasos hacia la soberanía digital. La Estrategia de diciembre aspira a reforzar la resiliencia de las cuatro cibercomunidades de la UE (el mercado, la diplomacia, la seguridad y la defensa) frente a las tensiones geopolíticas y los ciberataques contra las infraestructuras y los servicios que prestan. Para remediarlo, la Comisión confía en la regulación, la inversión y las políticas de cooperación con quienes compartan los principios e intereses europeos.

La profunda transformación del contexto digital ha obligado a la Comisión a revisar dos de sus directivas *estrella*: la de protección de las infraestructuras críticas (PIC) y la de seguridad de las redes y sistemas de servicios de información (NIS), que se han quedado desfasadas. Con la primera propuesta busca ampliar el concepto de "infraestructuras" que prestan servicios esenciales a la sociedad al más amplio de "entidades" en función del impacto que su interrupción cause en la economía o en la vida diaria de los ciudadanos, tanto de cada Estado como en el resto de la UE. Lo significativo de la propuesta es que obliga a los Estados miembros a identificar esas entidades críticas mediante estrategias y análisis de riesgos, que la Comisión se reserva el derecho de supervisar las entidades que afecten a otros Estados y que se ofrece a colaborar en la aplicación de las medidas necesarias para mejorar la resiliencia de estas entidades.

> "No existe autonomía sin dinero y la Comisión no se ha olvidado de invertir en el desarrollo de investigación, desarrollo e innovación de capacidades de ciberseguridad"

La segunda propuesta (NIS 2.0) amplía la regulación a nuevos sectores, como los postales, de alimentación, las Administraciones Públicas, las plataformas, los centros de datos, el espacio y los relacionados con la salud –una inclusión incentivada por la experiencia reciente de la pandemia–. También elimina la controvertida distinción entre los operadores de servicios esenciales y los proveedores de servicios digitales y la reemplaza por una segmentación en función de su trascendencia para el funcionamiento de la sociedad y economía digitales. Del mismo modo, reemplaza los criterios nacionales para designar los sujetos obligados al cumplimiento de la norma por una diferenciación establecida en función de su tamaño: afectará a todos los actores grandes y medianos e incluso a los pequeños si se demuestra su necesidad de inclusión. En definitiva, amplía y profundiza las medidas de la versión vigente de la NIS: de incentivar la adopción de medidas razonables de ciberseguridad a imponer el cumplimiento de las medidas, la declaración de incidentes y la cobertura de las cadenas de suministro completas; de apelar a la colaboración ante incidentes de importancia a centralizar la coordinación con estructuras y procedimientos vinculantes.

No existe autonomía sin dinero y la Comisión no se ha olvidado de invertir en el desarrollo de investigación, desarrollo e innovación de capacidades de ciberseguridad, tanto en los fondos comunes del Marco Financiero Plurianual ordinario como en los programas extraordinarios para la recuperación tras el impacto económico de la pandemia. Son inversiones estratégicas en la medida en que tratan de potenciar la base industrial y tecnológica de la ciberseguridad europea y articular ecosistemas europeos

que integren la ciberseguridad en la implantación de las nuevas tecnologías asociadas a la economía digital.

La agenda entrante

En 2021 se comenzarán a negociar o ejecutar las propuestas y medidas aprobadas por la Comisión en un escenario abierto a la colaboración interestatal y público-privada en los ámbitos de diálogo y trasparencia establecidos en los últimos años. Las medidas desbordan el anterior marco gubernamental de la seguridad para entrar en el más amplio de la seguridad económica, que incluye a más actores, no sólo en su condición de afectados por las nuevas medidas, sino también por el creciente papel protagonista de las asociaciones empresariales, profesionales o sociales europeas.

También se comenzará a aprobar la distribución de los fondos de inversión en capacidades de ciberseguridad, unos fondos que complementan, pero no sustituyen, a los fondos nacionales y que precisan una planificación individualizada para su inclusión entre los diversos programas. La selección depende de la Comisión, pero la presentación corresponde a los Estados miembros, que pueden coordinarla con sus ecosistemas industriales y de investigación o arriesgarse a ver como éstos se integran en candidaturas europeas con mayores posibilidades.

"Si se unen los puntos anteriores, aparece claramente –creemos– una creciente europeización de la ciberseguridad"

Siguen pendientes de resolución problemas como la aplicación de criterios comunes en relación con la seguridad de las redes 5G (léase la presencia o no de elementos y tecnologías chinas en ellas); la actualización de las medidas contra la desinformación y las amenazas híbridas; la adecuación de las herramientas policiales y judiciales para perseguir los delitos en la red, o el dilema entre privacidad y seguridad que plantea el cifrado, entre otros.

Si se unen los puntos anteriores, aparece claramente –creemos– una creciente europeización de la ciberseguridad (mayor protagonismo de la Comisión, ENISA y los órganos de gestión de crisis y coordinación operativa, así como de los fondos comunes, que implican una mayor participación del Parlamento Europeo). Una europeización en la que los actores no gubernamentales (asociaciones, foros, clústeres, ecosistemas, *hubs*, centros tecnológicos, aceleradoras, universidades…) asumen mayor protagonismo en el desarrollo de la soberanía digital frente a los Estados miembros. Esto no quiere decir que estos hayan perdido su liderazgo en los procesos de decisión y de regulación, sino que deben tener en cuenta los cambios de agenda y de tendencias para adaptar sus políticas de ciberseguridad. La creación del Foro Nacional de Ciberseguridad en España es un ejemplo de anticipación estratégica, tanto para desarrollar la agenda nacional como la agenda europea, en un contexto de cambio acelerado en el que aparecen nuevos retos mientras aún no se han resuelto los anteriores.