De los desafíos de la política de telecomunicaciones de la Unión Europea a los del ecosistema digital europeo

Editores

Miguel López-Coronado Sánchez-Fortún

Jorge Pérez Martínez

Cofinanciado por la Unión Europea

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por
la Unión Europea

DE LOS DESAFÍOS DE LA POLÍTICA DE TELECOMUNICACIONES DE LA UNIÓN EUROPEA A LOS DEL ECOSISTEMA DIGITAL EUROPEO

Cátedra **Jean Monnet**
> EUTELIS

Universidad
Europea
del Atlántico

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

Título: *De los desafíos de la política de telecomunicaciones de la Unión Europea a los del ecosistema digital europeo*

Editores:

© Miguel López-Coronado Sánchez-Fortún

© Jorge Pérez Martínez

Diseño y diagramación:

© Verónica Lombana Caro

Revisión de estilo:

© Nixon Yamid Rodríguez Baquero

ISBN: 978-84-127022-7-9

Esta publicación ha sido posible gracias al apoyo económico de la Universidad Europea del Atlántico y de la Unión Europea. Las noticias, los asertos y las opiniones contenidos en esta obra son de la exclusiva responsabilidad de los autores.

Prólogo

Europa se enfrenta hoy a un punto de inflexión. En un ecosistema digital global dominado por grandes plataformas tecnológicas, fundamentalmente estadounidenses y chinas, el continente europeo presenta una posición de debilidad relativa. La escasa presencia de campeones digitales propios y la dependencia tecnológica externa han dejado al descubierto una vulnerabilidad creciente, particularmente en contextos de crisis geopolítica como las guerras en Ucrania o en Oriente Próximo. Estos conflictos han evidenciado el grado de dependencia de Europa respecto a infraestructuras digitales foráneas y han reactivado el debate sobre su soberanía digital y su autonomía estratégica.

Sin embargo, Europa también dispone de activos importantes. Su liderazgo en regulación digital, la solidez de sus infraestructuras de telecomunicaciones y su firme apuesta por la sostenibilidad y la transición verde constituyen sus principales fortalezas. En este contexto, la digitalización se perfila como un instrumento esencial para transformar sectores clave como la energía, el transporte y la agricultura. La oportunidad de liderar la transición digital —sostenible, ética y segura— está al alcance si se acometen las reformas necesarias.

Este libro nace precisamente de la necesidad de entender, desde una mirada crítica y multidisciplinar, el papel de la política de telecomunicaciones de la Unión Europea en el desarrollo de la sociedad de la información. Se enmarca dentro del Proyecto EUTELIS, financiado por la Comisión Europea a través del programa Erasmus+, y coordinado por la Cátedra Jean Monnet de la Universidad Europea del Atlántico en colaboración con el Foro de la Gobernanza de Internet. Su carácter colectivo se traduce en la participación de expertos procedentes de universidades, administraciones públicas y empresas, tanto sénior como jóvenes, reflejando la diversidad de perspectivas necesarias para abordar un entorno tecnológico tan dinámico y complejo.

Con una mirada de largo plazo, la Comisión Europea lanzó en 2014 el proyecto del Mercado Único Digital, con el objetivo de eliminar las barreras internas al comercio y a los servicios digitales, y de fomentar una regulación común e innovadora. Esta apuesta ha permitido a la UE influir globalmente a través del denominado “efecto Bruselas”: al establecer estándares normativos ambiciosos —como el Reglamento General de Protección de Datos (RGPD), la Ley de Servicios Digitales (DSA), la Ley de Mercados Digitales (DMA) o la nueva Ley de Inteligencia Artificial—, Europa se ha convertido en un referente regulador más allá de sus fronteras.

Sin embargo, la paradoja es evidente: el único segmento del ecosistema digital que no está dominado por empresas no europeas —el de las telecomunicaciones— atraviesa una profunda crisis. Fragmentado en 27 mercados nacionales y sometido a una regulación que favorece la competencia sin garantizar sostenibilidad económica, los operadores europeos enfrentan serios problemas: bajo Ingreso Promedio por Usuario (ARPU), caída del Retorno sobre el Capital Empleado (ROCE), y una reducción dramática de su valor bursátil. Este debilitamiento financiero compromete su capacidad para abordar los desafíos tecnológicos inminentes, como la virtualización de redes, la nube perimetral, la inteligencia artificial o las redes abiertas.

Ante esta situación, la Comisión Europea ha reconocido en su Libro Blanco de 2024 la urgencia de transformar el modelo actual. Propone medidas para atraer inversión, mejorar la rentabilidad del sector y, sobre todo, construir un verdadero mercado único europeo de telecomunicaciones que supere la actual fragmentación. En esta misma línea, el informe Letta sobre el futuro del mercado único subraya la necesidad de culminar la integración de tres ámbitos clave: telecomunicaciones, finanzas y energía.

Esta obra aborda estos desafíos desde una perspectiva integral y estructurada. El libro se organiza en ocho capítulos que cubren los pilares fundamentales de la transformación digital europea:

1. **Evolución de la política de telecomunicaciones de la UE**, desde sus inicios hasta hoy, destacando sus logros en eficiencia, accesibilidad y competitividad.
2. **Futuro del sector**, analizando las nuevas tecnologías, su impacto económico, y la necesidad de una regulación que responda a esta transformación.
3. **Ecosistema digital global**, con una mirada a los actores, las tendencias y los desafíos tecnológicos emergentes como la inteligencia artificial, la computación cuántica o los semiconductores.
4. **Geopolítica digital**, explorando la posición estratégica de Europa en un mundo multipolar y sus aspiraciones de autonomía tecnológica.
5. **Ciberdefensa europea**, abordando el ciberespacio como nuevo escenario de conflicto y la necesidad de una respuesta coordinada desde la defensa.
6. **Seguridad de redes**, frente a amenazas crecientes de delincuencia especializada y vulnerabilidades sistémicas.
7. **Regulación del ecosistema digital**, con un análisis de los principales instrumentos normativos europeos y su influencia global.
8. **Impacto de la inteligencia artificial en los derechos ciudadanos**, un tema clave para el futuro de la gobernanza digital democrática.

La ambición de este libro es doble: ser una fuente rigurosa de información para especialistas, legisladores y profesionales del sector y, al mismo tiempo, ofrecer una guía reflexiva e inspiradora para quienes se interesan por el futuro digital de Europa. En un momento donde las decisiones tecnológicas son también decisiones políticas, creemos que este trabajo contribuye a entender los dilemas, riesgos y oportunidades que marcarán el rumbo de una Europa que quiere seguir siendo relevante, justa y soberana en el siglo XXI.

Miguel López-Coronado Sánchez-Fortún

Jorge Pérez Martínez

Autores

Política de Telecomunicaciones de la Unión Europea. Fases: desde el monopolio hasta las Comunicaciones Electrónicas. La regulación mediante directivas	Miguel López-Coronado Sánchez-Fortún Fermín Fontecha
El Futuro de las Telecomunicaciones Europeas	Juan Luis Redondo Maíllo
Evolución y Tendencias del Ecosistema Digital Global	Jorge Pérez Martínez Pilar Rodríguez Pita
Geopolítica Digital. La Autonomía Digital Estratégica de la UE	Emilio García García
El Ciberespacio como nuevo escenario de conflictos. Una visión en el marco de la defensa europea	Fernando Davara Rodríguez
Seguridad en las Redes	Xavier Larriva-Novo Carmen Sánchez-Zas
La Regulación Europea del Ecosistema Digital. El Reglamento General de Protección de Datos (RGPD), La Ley de Servicios Digitales (DSA), la Ley de Mercados Digitales (DMA) y la Ley de Inteligencia Artificial	Pilar Rodríguez Pita Jorge Pérez Martínez
Prospectiva sobre el impacto de la inteligencia artificial en los derechos de los ciudadanos	Moisés Barrio Andrés

Miguel López-Coronado Sánchez-Fortún

Es Ingeniero y Doctor Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid. Ha sido Profesor Titular en la Universidad Politécnica de Madrid y Catedrático de Universidad por las Universidades de Santiago de Compostela, de Vigo y de Valladolid. Actualmente es Catedrático Emérito en la Universidad Europea del Atlántico.

Ha desarrollado su docencia e investigación en el campo de tecnología electrónica y la Sociedad de Información siendo Coordinador del Grupo de Investigación Reconocido de la UVA Sociedad de la Información en telemedicina, eSalud y regulación de las telecomunicaciones. Ha generado múltiples direcciones de Tesis Doctorales, publicaciones científicas en revistas indexadas y comunicaciones a Congresos de reconocida solvencia.

Ha realizado funciones de gestión académica, como director de escuela y de departamento facilitando la implantación de titulaciones y de estudios de doctorado.

Su participación en la gestión de I+D+i se ha centrado en la dirección y participación de proyectos de investigación, en la creación y gestión del Centro Tecnológico para el Desarrollo de las Telecomunicaciones de Castilla y León (CEDETEL); asimismo en la creación y gestión de varias Cátedras de Empresas en la Escuela Técnica Superior de Ingenieros de Telecomunicación de Universidad de Valladolid.

Es miembro del Instituto de Telecomunicaciones.

Es evaluador de revistas JCR y de congresos, así como de proyectos de investigación en la Agencia Nacional de Evaluación y Prospectiva (ANEP) y en la Agencia Nacional de Investigación (AEI).

Ha formado parte de ocho comités científicos, técnicos o de asesoramiento.

Ha sido miembro del Consejo de las Telecomunicaciones de Castilla y León, participando como director técnico de la ponencia de telemedicina y miembro del comité de elaboración del plan director de infraestructuras y servicios de las telecomunicaciones.

También ha desarrollado su carrera en el ámbito privado, habiendo sido director general de RETECAL S.A. y consejero delegado de Divisa IT S.A., entre otros puestos.

Actualmente es Chair en la Universidad Europea del Atlántico de la Cátedra Jean Monnet “Política de Telecomunicaciones de la Unión Europea y Sociedad de la Información - Proyecto EUTELIS” otorgado por la Comisión Europea a la Universidad Europea del Atlántico en el Marco de las Acciones Jean Monnet, dentro del programa ERASMUS+.

Fermín Fontecha

Fermín es Ingeniero de Telecomunicación por la ETSI de Telecomunicación de Valladolid. Además, posee otras titulaciones universitarias complementarias por la UNED (especialista universitario en consultoría de empresa) y por la Universidad de Alcalá (experto en dirección y gestión de la información y sus tecnologías), además de un MBA en internacionalización de empresas por el ICEX, y múltiples certificaciones de los fabricantes más representativos de las TIC.

Con un perfil polifacético, en sus treinta años de vida profesional ha trabajado en la mayoría de los actores integrantes del mercado de las Tecnologías de la Información y las Telecomunicaciones, incluyendo Centros de I+D, fabricantes, operadores, integradores y la Administración Pública. Ha sido emprendedor y empresario, y ha residido en España, Inglaterra y Suiza, desarrollando sus tareas profesionales en Europa y Asia-Pacífico.

En su última etapa, ha desarrollado su labor en la Administración Pública española durante tres años como consultor tecnológico para la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, concretamente en la Subdirección General de Ordenación de las Telecomunicaciones y ha pasado a ejercer dicha labor en el Ministerio de Defensa, puesto que ocupa desde enero de 2025.

Juan Luis Redondo Maíllo

Licenciado en Informática por la Universidad Politécnica de Madrid, Máster en Computer Science por la Universidad de Illinois Urbana-Champaign y Máster en Negocios de Telecomunicaciones por el Instituto de Empresa.

Una carrera profesional desarrollada en su mayor parte en el sector de las telecomunicaciones. Tras volver de Estados Unidos, inicia su carrera profesional en consultoría en Atos ODS, para después desempeñar durante 10 años diferentes puestos ligados al desarrollo de proyectos software en Telefónica I+D, la compañía de Telefónica centrada en la investigación, el desarrollo y la innovación.

Continúa su carrera profesional en puestos de dirección en el área de estudios de Red.es, ligada al impulso de programas de fomento de la Sociedad de la Información.

Tras esta etapa, desempeñó diferentes puestos en el área de Estrategia de Telefónica España antes de incorporarse a Telefónica S.A, para crear e impulsar la Oficina Internacional de Telefónica S.A., donde se desarrollan las políticas de Telefónica relacionadas con Internet y el mundo digital.

En los últimos 10 años ha desempeñado diferentes puestos de dirección en las áreas de Regulación, Políticas Públicas y Asuntos Públicos de Telefónica S.A. Actualmente director de Políticas Públicas Digitales en Telefónica S.A.

Desempeñó también diferentes puestos en organismos internacionales ligados a las políticas públicas digitales, como vicepresidente en Business en OCDE (BIAC) del comité de política regulatoria y gobernanza, y vicepresidente del comité global de economía digital de la Cámara de Comercio Internacional (ICC).

Actualmente es Profesor Asociado en la Escuela de Ingeniería Superior de Telecomunicaciones en la Universidad Politécnica de Madrid.

Jorge Pérez Martínez

Es Ingeniero y Doctor Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid (UPM) y Licenciado en Ciencias Políticas y Sociología por la Universidad Complutense de Madrid. En la actualidad es Catedrático Emérito en la ETSI de Telecomunicación de la UPM, desarrollando sus funciones docentes e investigadoras en el Grupo de Investigación de las Tecnologías de la Información y las Comunicaciones (GTIC) del Departamento de Señales, Sistemas y Radiocomunicaciones (SSR) de la UPM, que fundó en 1995. Es director ejecutivo de Fundetel; codirector de la Cátedra de Economía, Sociedad y Transformación Digital de Telefónica; y coordinador del Foro para la Gobernanza de Internet en España (IGF Spain).

De junio de 1990 a febrero de 1999 fue Decano del Colegio Oficial de Ingenieros de Telecomunicación y presidente de la Asociación Española de Ingenieros de Telecomunicación.

Fue miembro de su Consejo del Colegio hasta 2009.

De septiembre de 1991 a septiembre de 1993 fue director del Departamento de Prospectiva Tecnológica de FUNDESCO (denominación de la Fundación Telefónica en aquel momento).

Desde su creación en 1996 hasta marzo de 2003 fue vocal del Consejo Asesor de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología y miembro de su Comisión Permanente.

De septiembre de 2003 a junio de 2004 fue director general para el desarrollo de la Sociedad de la Información en el Ministerio de Ciencia y Tecnología y consejero de los Consejos de Administración del CDTI y de la Entidad Pública Empresarial Red.es.

De diciembre de 2007 a agosto de 2015 fue director de la Cátedra Red.es en la UPM desde donde asesoraba a la Secretaría de Estado de Telecomunicaciones y para el Desarrollo de la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio.

De agosto de 2015 a octubre de 2018 se incorpora en comisión de servicio a la entidad empresarial Red.es como director de Economía Digital y director del Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información.

En el ámbito empresarial, ha sido presidente y fundador de la Consultora Symmachia, consejero de TTT e Infoglobal y asesor de los comités de dirección de IKUSI, CEPREDE y Cable AML.

Ha sido Patrono fundador y vicepresidente de las Fundaciones DINTEL y ONG Solidarios Profesionales. Actualmente es miembro del Consejo Asesor de CITAC Fundación Diálogos y Patrono de las Fundaciones Fundetel, España Digital.

Fernando Davara Rodríguez

General de Brigada de Artillería (Retirado), Diplomado de Estado Mayor, Físico (Especialidad de Automática e Informática) y Doctor “cum laude” en Ingeniería Informática.

Más de 40 años de trabajo e investigación en los dominios de la Ciberseguridad, Sistemas espaciales y sus aplicaciones, sociedad digital, inteligencia artificial, economía y competitividad, seguridad y defensa, etc.

Autor de numerosos trabajos y ponente habitual de seminarios y coloquios (nacionales e internacionales), ha llevado a cabo actividades investigadoras y de formación y ocupado diversos cargos nacionales y extranjeros, entre ellos seis años como director del Centro de Satélites de la Unión Europea (EUSC).

Actualmente, entre otros, es Presidente de la Fundación “España Digital”, Secretario del Consejo Asesor del Clúster de Ciberseguridad de Madrid, Miembro del Consejo Asesor del Clúster de la Industria de Defensa, Miembro del Consejo Asesor del IGFS (Foro de la Gobernanza de Internet en España), Miembro de la Comisión de Impulso del Día de Internet, Académico de la Academia de la Diplomacia del Reino de España, vicepresidente del Ateneo de Valladolid y miembro de la Asociación Española de Militares Escritores.

En marzo de 2024 recibió la medalla al Mérito de la Ciberdefensa, de nueva creación, como “reconocimiento a su trabajo, tanto profesional como personal, en la Ciberdefensa y en la Ciberseguridad de nuestra Nación, sus gentes y sus intereses”.

Emilio García García

Coautor del libro “Chips y Poder”. En el servicio público desde 2005 y exdirector de gabinete de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, actualmente adscrito al Instituto de Astrofísica de Canarias (IAC). Analista de políticas digitales en medios como Cinco Días y Agenda Pública. Miembro del Consejo Asesor de AESEMI (Asociación Española de la Industria de Semiconductores) y ha colaborado con la Fundación Alternativas y el Real Instituto Elcano. Profesional del sector tecnológico desde 1989.

Pilar Rodríguez Pita

Es estudiante de doctorado en la Universidad Politécnica de Madrid donde obtuvo los títulos de Grado y Máster en Ingeniería de Telecomunicaciones. Se ha especializado en temas relacionados con la soberanía digital y la regulación digital europea, publicando varios artículos sobre el tema en diferentes revistas académicas. Adicionalmente, desde 2022 coordina la rama joven del Foro de Gobernanza de Internet en España, organizando eventos tanto a nivel nacional como internacional.

Carmen Sánchez-Zas

Recibió su doctorado en Ingeniería Telemática por la Universidad Politécnica de Madrid (UPM) en 2024. Actualmente trabaja como Profesora Ayudante Doctora en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, donde también ejerce como investigadora en el grupo de Redes y Servicio de Telecomunicación e Internet. Acumula una amplia experiencia en investigación adquirida a través de su participación en proyectos nacionales y europeos. Como resultado de su actividad investigadora, ha publicado más de quince artículos en conferencias y revistas de primer nivel. Sus intereses de investigación actuales giran en torno a la gestión dinámica de riesgos, centrándose en seguridad de la red, el soporte a la toma de decisiones, inteligencia artificial y conciencia cibersituacional.

Xavier Larriva-Novo

Es Profesor Permanente Laboral en la Universidad Politécnica de Madrid (UPM). Recibió Máster Universitario en Ciberseguridad en 2018 y Doctorado en Ingeniería de Sistemas Telemáticos en 2022, ambas por la UPM. Ha estado involucrado en varios proyectos de investigación financiados con fondos públicos europeos y españoles relacionados con sistemas de red, gestión, aplicación y diseño de servicios además de la seguridad de redes, aprendizaje automático y computación de alto rendimiento, así como diferentes proyectos nacionales orientados a ciberseguridad y defensa. Es autor de más de 30 publicaciones técnicas en revistas y congresos nacionales e internacionales. Ha obtenido diversos premios, entre ellos la mejor tesis doctoral otorgada por la cátedra de la UPM con el CESEDEN (Centro de Estudios de la Defensa Nacional), Ingeniero General D. Antonio Remón y Zarco del Valle y el premio extraordinario de doctorado otorgado por la Universidad Politécnica de Madrid.

Moisés Barrio Andrés

En 1992, a sus 11 años, fundó IDESOFT, empresa fabricante de software y de soluciones tecnológicas y de ciberseguridad que fue pionera en Internet. Licenciado en Derecho por ICADE. Máster en Investigación en Ciencias Jurídicas por ICADE, ESADE y Deusto. Doctor en Derecho por la Universidad Carlos III de Madrid con sobresaliente *cum laude*. Letrado del Consejo de Estado desde 2009 con el número 1 de la promoción. Es delegado de Protección de Datos del mismo. Ha realizado estudios de postgrado en la Universidad de Harvard y en la London School of Economics.

Profesor de Derecho Digital en las Universidades Carlos III de Madrid, ICADE, UNED, San Pablo CEU y Complutense de Madrid, y en el Ilustre Colegio de Abogados de Madrid. Director del posgrado en *legaltech* y transformación digital (DAELT) en la Escuela de Práctica Jurídica de la Universidad Complutense de Madrid, y codirector del postgrado en IA y Derecho en la misma universidad. Pertenece al Consejo Asesor de Aranzadi LA LEY (antiguo consejo editorial). Codirector de la Revista Aranzadi LA LEY Derecho Digital e Innovación. Miembro de la Real Academia de Jurisprudencia y Legislación. Asesor de distintos gobiernos, tanto en España, la Unión Europea y otros Estados, en materias de Derecho de Internet y transformación digital.

Entre otras normas, ha participado en la elaboración de la Carta de Derechos digitales o del Reglamento europeo de IA. Pertenece al grupo de expertos sobre ciberpolítica del Real Instituto Elcano, y al Foro Nacional de Ciberseguridad. Forma parte de diversos proyectos de investigación de ámbito nacional e internacional. Es autor hasta la fecha de dieciocho libros individuales sobre Internet, Derecho digital, tecnologías disruptivas (IoT, robótica, inteligencia artificial, *blockchain*, criptoactivos, coches autónomos, criptoactivos…), *legaltech*, derechos digitales, ciberdelincuencia, ciberderecho, propiedad intelectual y regulación digital.

Ha dirigido otros ocho libros al respecto. Ha publicado también más de 170 capítulos de libros, artículos en revistas y otras obras especializadas. Es colaborador habitual de El País y El País Retina, Cinco Días, El Confidencial, Confilegal, BlogAbogacía y otros medios de comunicación, como jurista experto en derecho digital y protección de datos. En 2018 recibió el Premio ENATIC a la investigación jurídica en Derecho digital.

Gran Cruz de la Orden de San Raimundo de Peñafort al Cuerpo de Letrados del Consejo de Estado. Asiduo ponente y conferenciante en diversos congresos, jornadas y encuentros internacionales y españoles.

Índice

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

1

Política de telecomunicaciones de la Unión Europea. Fases: desde el monopolio hasta las comunicaciones electrónicas. La regulación mediante directivas

Miguel López-Coronado Sánchez-Fortún
Fermín Fontecha

En este capítulo vamos a plantear la trayectoria de la Política de Telecomunicaciones en la Unión Europea desde la situación de monopolio estatal hasta la actual, con su liberalización en 1998.

La Política de Telecomunicaciones de la Unión Europea ha estado caracterizada por el carácter privado de las operadoras de telecomunicaciones, a partir de su liberalización. Se ha pasado de una situación de monopolio estatal, o empresa controlada por el estado, como en el caso español, Telefónica, a una privatización, en competencia, de estos operadores incumbentes.

El fin de la generación de competencia era dar lugar a unos precios adecuados y a una profunda modernización de las tecnologías relacionadas con las telecomunicaciones, dado su constante progreso. Por ello, se impulsó la creación de nuevos operadores y, a la vez que se abría el mercado a operadoras de diferentes estados miembros. Todo ello con la idea de generar un mercado único europeo.

Junto con otras áreas de interés económico, como la energética y la financiera, se han regulado por Directivas europeas[1]. No obstante, el hecho de transponer dichas directivas[2] a la legislación de cada Estado miembro, no ha contribuido, en muchos casos, favorablemente a la formación de un mercado único de las telecomunicaciones.

El mercado único requiere, idealmente, de normalizaciones y homologaciones comunes a todos los estados miembros, con base en las organizaciones internacionales de telecomunicaciones y a organismos potenciados o creados por la CEE (hoy UE) para tal fin.

---

1. Los cinco tipos de actos legislativos con los que cuenta la UE para legislar son los siguientes:
    1. *Reglamentos*: son actos legislativos vinculantes. Tienen un alcance general, son obligatorios en todos sus elementos y directamente aplicables en cada estado miembro.
    2. *Directivas*: son actos legislativos en los cuales se establecen objetivos que todos los países de la UE deben cumplir. Sin embargo, corresponde a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos.
    3. *Decisiones*: son normas obligatorias en todos sus elementos, vinculantes para aquellos a quienes se dirigen (un país de la UE o una empresa concreta) y son directamente aplicables.
    4. *Recomendaciones*: no son normas jurídicas, son actos no vinculantes. Son instrumentos de acción indirecta para armonizar las legislaciones, que difieren de la directiva únicamente por la ausencia del carácter de obligatoriedad.
    5. *Dictámenes*: son instrumentos que permiten a las instituciones hacer declaraciones u opiniones de manera no vinculante, es decir, sin imponer obligaciones legales a quienes se dirigen. Pueden emitirlos las principales instituciones de la UE (*Comisión*, *Consejo* y *Parlamento*), el *Comité de las Regiones* y el *Comité Económico y Social Europeo*. Mientras se elabora la legislación, los comités emiten dictámenes desde su propio punto de vista, regional o económico y social.
2. Los Estados miembros las transponen (incorporan a las legislaciones nacionales), adquiriendo rango de ley en los Estados miembros. Por tanto, corresponde a cada Estado miembro formular sus propias leyes para determinar cómo aplicar estas normas.

TRANSPOSICIÓN DE DIRECTIVAS COMUNITARIAS AL SISTEMA JURÍDICO ESPAÑOL

- Linde Paniagua, E. y Pilar Mellada. Iniciación al Derecho de la Unión Europea. COLEX 2003.
- Linde Paniagua, E. y otros. Derecho de la Unión Europea, Vol. I, Editorial Marcial Pons. Madrid, 1995.
- Puente Egido, J. Lecciones de Derecho Internacional Público. Editorial Dykinson.
- Palacio González, J. El sistema comunitario de fuentes del derecho y su articulación con los ordenamientos nacionales. Gobierno Vasco, Vitoria, 1991.
- Gamir Meade, R. Un enfoque práctico desde la óptica de técnica normativa de las operaciones de transposición de Directivas comunitarias. Revista del Poder Judicial, nº 49.
- Mangas Martín, A. y Liñan Nogeras, D.J., Instituciones y Derecho de la Unión Europea.

Con anterioridad a la mencionada liberalización en 1998, se buscaba garantizar dicha liberalización, la armonización e interconexión introduciendo mecanismos correctores a la Libre Competencia, para compensar posibles inconvenientes a la misma.

Fue a partir de 1998 cuando se fue produciendo, con base en la experiencia y las necesidades de una adecuación de la política de telecomunicaciones y gracias a la evolución del mercado y de las nuevas tecnologías, que se desarrollaban a considerable velocidad, el desarrollo de una legislación de actualización de las Directivas, en las que se incorporó el término comunicaciones electrónicas, más amplio que el de telecomunicaciones.

Y gracias a esa libre competencia, fueron las necesidades del mercado las que exigieron ir actualizando dicha política. De esta forma, se realizó una primera revisión, conocida como el paquete Telecom 2002, en el que, a partir de las exigencias introducidas por este paquete, se realizaron las consultas pertinentes a las partes interesadas del sector, e incorporándose la experiencia acumulada hasta ese momento en otra actualización mediante el denominado paquete Telecom 2009.

Además, la aparición de Internet, y su paradigma, con su acción sobre redes y servicios, requiriendo de una política de Banda Ancha para el Ecosistema del Sector Digital.

Por otro lado, no podemos obviar el problema planteado por la crisis económica de 2008, que dio lugar a las políticas digitales, integradoras y sostenibles, lanzadas por la Unión Europea a nivel empresarial y social. "Las décadas digitales", requerían de redes de muy alta capacidad (gracias a la introducción masiva de fibra óptica), y de una política del espectro radioeléctrico que facilitase, entre otros sistemas, la telefonía móvil. Para garantizar la calidad del ecosistema digital se han introducido reglamentos sobre la protección de datos, servicios digitales, mercados digitales y, como ejemplo de tecnologías de alto rendimiento, el de inteligencia artificial.

En la actualidad, el Código Europeo de las Comunicaciones Electrónicas pretende canalizar todas estas y futuras necesidades, debiendo evolucionar hacia una normativa que, de acuerdo con las consultas realizadas, el Libro Blanco, los Informes Letta y Draghi, persiguen conseguir un mercado único en un momento económico y político muy crítico, mediante una atractiva y confiable financiación, que permita a la Unión Europea seguir siendo un actor relevante en el ecosistema digital, en competencia con EE. UU. y China, y a la espera de la Ley de Redes Digitales en que cristalice todo lo expuesto.

Para explicar convenientemente a los lectores toda esta trayectoria, el capítulo lo vamos a dividir en apartados que faciliten la comprensión de esta evolución hasta su estado actual, así como de las herramientas institucionales utilizadas y de los tratados más importantes que han ido cimentando la política europea en este sector.

1.1. TRAYECTORIA DE LA POLÍTICA DE TELECOMUNICACIONES DE LA UNIÓN EUROPEA

La Política de Telecomunicaciones de la Unión Europea es un tema amplio y clave en la regulación del mercado digital y las infraestructuras de comunicación en Europa.

1.1.1. Orígenes de la política de telecomunicaciones

Las instituciones de la Unión Europea, en ese momento denominada Comunidad Económica Europea, pronto se dieron cuenta de la importancia de las Telecomunicaciones para el desarrollo económico, cultural y social de los estados miembros, así como de la necesidad de una evolución armónica que garantizase normativas comunes que permitiesen la consecución de ese

mercado único anhelado, eje principal las políticas económicas, culturales y sociales europeas.

Es precisamente a finales de los años sesenta donde se empieza a hablar de telecomunicaciones dentro de las políticas de tecnología electrónica (aunque no siempre de forma prioritaria, por no entrar en conflicto con los tratados de la Comunidad Económica Europea), concretándose con el desarrollo del Acta Única Europea.

La decisión de la cumbre de La Haya de 1969 de afrontar nuevas políticas, con el objetivo de ir hacia una Europa comunitaria, generó la necesidad de dictaminar también en el campo de las nuevas tecnologías de la información, remontándose las primeras actuaciones a 1967 (1) y las primeras propuestas de la Comisión a 1980.

Los primeros pasos que condujeron al inicio de la Política de Telecomunicaciones de la Unión Europea se dieron mediante informes de diversos grupos de trabajo, en los que se planteaba constantemente el estado del sector de las Telecomunicaciones a lo largo de los años 70 y de los 80, pese a que se hacía de manera indirecta en algunos casos. En dichos informes, se mostraba el retraso comparativo frente a los competidores directos (EE. UU. y Japón), tanto en facturación como en innovación, destacando principalmente el mercado de los semiconductores, que, al ser suministrados por ellos para atender la demanda europea, dieron lugar a que Europa careciera de capacidad para innovar y competir con ellos…

Aquellos informes también mostraban carencias en la prestación de servicios, de sistemas de telecomunicación y de las industrias suministradoras afectadas, fruto de la falta de volumen de unas inversiones adecuadas, y como consecuencia de un mercado constreñido a los de cada Estado miembro por separado. También, aparecieron nuevas necesidades en transmisión de datos e imágenes, todo ello en un mundo cambiante social y económicamente, característica de las sociedades modernas del momento.

Aquella situación planteaba claramente la necesidad de ampliar mercados, cuya primera etapa sería un mercado único europeo del sector de las telecomunicaciones. Pero dicho mercado requería de normalización y homologación aceptadas y armonizadas por los estados miembros. Para ello era necesario basarse en las instituciones regulatorias internacionales (2), favoreciendo un crecimiento armonioso en cuanto a la normalización de los equipos.

Es entonces cuando la Comunidad plantea establecer acciones piloto en diferentes aspectos de telecomunicaciones, partiendo de los estudios prospectivos COST (3) (4), para facilitar ese mercado único. Uno de los programas más importantes de esta fase fue COST 11, lanzado en 1977 dentro del marco del programa de cooperación científica y técnica (COST, por sus siglas en inglés). Este programa buscó mejorar la interconexión de las redes de telecomunicaciones en Europa, promoviendo estándares comunes y explorando la viabilidad de sistemas de comunicación más avanzados.

Estos estudios llevados a cabo a requerimiento de la Comisión, promovían la creación de EURONET, una Red europea para realizar, de la forma más rápida y económica posible, la conexión a todos los interesados de la Comunidad. La propuesta surgió de las administraciones nacionales de PTT reunidas en el CSTD (Comité Especial para la Transmisión de Datos) y bajo el patrocinio de aquella.

Digamos que aquella fue la primera vez que una simple red de transmisión de información, con tecnología de conmutación de paquetes, se creaba en Europa (5).

Mediante la comunicación de la Comisión de 26/11/1979 (6), se plasmaron las concreciones realizadas por los jefes de Estado y de Gobierno reunidos en Bonn en julio de 1978, reconociendo la necesidad de identificar nuevas formas de crecimiento y empleo más allá de las industrias tradicionales como el acero, el carbón, la construcción de barcos o los textiles. De igual forma, en su reunión del CE de Estrasburgo, confirmaron que la información compleja y dinámica de las industrias basadas en las nuevas tecnologías electrónicas ofrecían una fuente de crecimiento económico y de desarrollo social, dando un paso definitivo a la necesidad de desarrollar una política de telecomunicaciones en la comunidad.

Mientras, en la sociedad se estaba produciendo la introducción de nuevas tecnologías electrónicas que estaban evolucionando las redes de información, y prometían transformar la producción industrial y el trabajo en las oficinas, reduciendo costes y agilizando servicios. Eran dos revoluciones tecnológicas: las telecomunicaciones digitales y las tecnologías de la información y computación (transmisión de información sobre nuevos soportes: fibra óptica, telefonía móvil y redes de satélite).

La comunidad empezó a abordar el problema a finales de 1979, sin crear instrumentos financieros, pero urgiendo a los actores institucionales a movilizar y coordinar los esfuerzos realizados entre los estados miembros (7).

Esa situación puso de manifiesto que:

- Las nuevas infraestructuras de telecomunicaciones eran imprescindibles para los nuevos servicios, que iban desde el correo electrónico a videotexto, y la transmisión de datos ofertada por los modernos soportes de transmisión (fibra óptica, satélites), conjugadas con la conmutación y la transmisión digital.
- Los nuevos servicios debían adquirir un carácter más transnacional, en el mundo de las empresas multinacionales, del comercio y de la industria, representando un mercado considerable para esas nuevas aplicaciones.
- Constituían una infraestructura esencial para el desarrollo de la economía europea, ofrecían una solución económica a los transportes individuales, también para el desarrollo regional y el establecimiento de comunicaciones más rápidas y menos onerosas entre personas dentro de Europa.

El desarrollo en Europa de una red de telecomunicaciones competitiva y económica ofrecía una amplia gama de nuevos servicios telemáticos, así como un mercado comunitario abierto a la industria europea, contribuyendo al boom de actividades económicas de la comunidad en una época donde la electrónica digital juega un papel esencial.

A partir de ese momento se multiplicaron las acciones orientadas a potenciar las telecomunicaciones en la comunidad. Tanto el Parlamento Europeo 11/05/1982 (8); 03/03/1984 (11), como el Consejo 28/03/1983-03/189/CEE (9); COM(83) 329 final 9/06/1983 (10); 18/05/1984 COM(84)277 (12).

Los pasos a seguidos por la CEE en temas de Telecomunicación pasaron a centrarse en el estado de la misma, armonización, normativas y el desarrollo de regiones desfavorecidas, con programas para potenciar infraestructuras y servicios mediante directivas, recomendaciones, decisiones y reglamentos del Consejo y de la Comisión (13) (14) (15) (16) (17) (18) (19) (20).

También se apoyaron en consultas, y con las publicaciones de Libros Verdes o Blanco[3] según el motivo a plantear (21).

1.1.2. Primeros desarrollos de la liberalización, armonización y normalización (1987-1992)

En este período se trataba de desarrollar el mercado único de los equipos y servicios de telecomunicaciones, y tal tarea precisaba de dos enérgicas acciones: la apertura de los mercados y la imposición de la utilización de normas técnicas comunes en toda la Unión.

El primero de los objetivos se alcanzó con la adopción de la Directiva 88/301 (22) de la Comisión, por la que se abría a la competencia los mercados de equipos terminales de telecomunicaciones, que, pese a los retrasos de algunos estados miembros mostrando reticencia a abandonar el monopolio, acabó entrando en vigor en 1991.

Sin embargo, la consecución del segundo de los objetivos llevó toda una década de trabajo,

3. En el caso del **Libro Verde**, es un sistema para recopilar información para conocer qué se opina sobre el área que trate. Tras su publicación, puede que se continúe el trabajo con un **Libro Blanco**. El **Libro Blanco** ya contiene propuestas concretas del Gobierno y significa que existe una intención de legislar sobre el tema.

ya que la garantía del interfuncionamiento de los terminales, de las redes y de los servicios de telecomunicaciones en la Comunidad Económica Europea que había mantenido el sector durante un siglo de monopolios, debía de quedar garantizado cuando este estuviera en libre competencia.

En ese sentido había comenzado a actuar la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT) con la elaboración de Normas Europeas de Telecomunicaciones, con ese objetivo también se creó el Instituto Europeo de Normas de Telecomunicaciones (ETSI), y en esa dirección actuaron las instituciones europeas adoptando reglamentaciones técnicas comunes.

Fue la estrategia de 1987 la que inició verdaderamente el proceso de liberalización de los mercados de las telecomunicaciones en la Unión Europea; primero el de los equipos, y posteriormente el de los servicios. Es, por tanto, en el marco de esta estrategia, en el que la Política de Normalización y Certificación adquirió su dimensión, voluntaria u obligatoria, partiendo de las bases creadas en los años anteriores.

Tal y como figuraba en la Directiva 91/263/CEE (23), la obligatoriedad de estas normas iba a establecerse a través de la aprobación de Reglamentaciones Técnicas Comunes (CTR), adoptadas con todas las garantías necesarias mediante Decisiones de la Comisión.

Como consecuencia de ello, las legislaciones nacionales iban a tener que dar automáticamente el certificado de homologación nacional si se cumplían los requisitos exigidos. Para ello, la demostración del cumplimiento de dichos requisitos iba a acreditarse mediante un Certificado de Conformidad de su cumplimiento, que iba a dar derecho a la utilización del marcado CE (Conformité Européenne).

Otro de los aspectos a destacar como parte de la Política de Normalización de la Unión Europea es el que hacía referencia a la utilización de las normas técnicas en el marco de la Política de Armonización y de su desarrollo a través de la Oferta de Red Abierta (ONP), (Directiva 92/44/CEE (24)).

En aquellos casos como el de la Red Digital de Servicios Integrados (RDSI) y las Redes de Paquetes de datos (en los que las actuaciones ONP quedaron en simples Recomendaciones del Consejo), cualquier referencia a las normas a utilizar en estos servicios no pasó de la categoría de recomendación. Únicamente en el caso de la Directiva ONP de las Líneas alquiladas, la referencia a las normas técnicas pasó a ser un requisito de obligado cumplimiento.

A partir de este momento la normalización se extendió al buen funcionamiento del sector de cara a la libre competencia tanto en servicios como en infraestructuras, obligatoria para garantizar la protección de personas e instalaciones o bien para asegurar el interfuncionamiento y la interoperabilidad de determinados servicios.

Destacamos, a continuación, algunos aspectos prioritarios para la liberalización:

- La Directiva 97/33/CE (25) de Interconexión hacía una referencia explícita a las normas técnicas, y eran obligatorias las referentes a la seguridad de la red, el mantenimiento de la integridad de la red, la interoperabilidad de los servicios y la protección de los datos.
- La interoperabilidad de los servicios tenía carácter obligatorio.
- Referente a la telefonía vocal, la Directiva sobre aplicación de la ONP hacía referencia a las normas técnicas en diferentes aspectos, como eran los terminales, las interconexiones, la calidad del servicio, y los servicios adicionales de la red.
- Referente a los terminales de telecomunicaciones que podrían conectarse a las redes públicas de telefonía vocal, era evidente que dichas redes iban a quedar obligadas a garantizar el correcto funcionamiento de los terminales, dada la existencia de una fuerte reglamentación comunitaria en esta materia. referente a la calidad de los servicios ofrecidos a los usuarios, el artículo 12 lo abordaba, y en el Anexo III aparecía la relación de normas técnicas de ETSI que se utilizarían para la medida de dichos parámetros de calidad.

En el caso del Reino de España, una vez dentro de la CEE, ajustó su legislación entre otras Leyes la 31/1987 de Ordenación de las Telecomunicaciones y el Real Decreto 970/1991, por el que se establece la composición y régimen de funcionamiento del Consejo Asesor de Telecomunicaciones.

1.1.3. Desarrollo de la liberalización, armonización e interconexión y los mecanismos correctores a la libre competencia. El servicio universal (1992-1997)

Sin embargo, no fue hasta finales de los años ochenta, tras iniciarse el proceso de liberalización del sector en Estados Unidos con la decisión de romper el monopolio de AT&T en 1982, cuando en 1987 la Comisión abrió un debate entre todas las partes interesadas (26), lo que llevó al inicio del proceso de liberalización y a la posterior publicación de las normativas dirigidas a lograr este objetivo.

A raíz de esta liberalización parcial (que excluyó la telefonía vocal y otros servicios que constituían la mayor parte del mercado de las telecomunicaciones), la Comisión Europea propuso la liberalización total de los servicios de telecomunicaciones en 1993 mediante la comisión de Asuntos Económicos y Monetarios y de Política Industrial, de 15/10/1994 A4-0073/94 (COM(94)0347 Final-C4-0113/94), respondiendo a: sobre la recomendación al Consejo Europeo "Europa y la sociedad global de la información" (27) y sobre la comunicación de la Comisión de las Comunidades Europeas "Europa en marcha hacia la sociedad de la información. En su plan de actuación" (28) se plantean infinidad de temas de gran trascendencia en el desarrollo de la sociedad de la información: desde su propia definición, a los aspectos de desarrollo de infraestructuras, servicios, temas de liberalización, de aplicaciones básicas de sanidad, educación y formación, trabajo a distancia…, poniendo sobre la palestra los posibles inconvenientes y ventajas del hecho mismo de la utilización de las tecnologías de información y de las telecomunicaciones, que en todo momento deberían estar suficientemente expandidas, con precios económicos, con total accesibilidad.

Para el desarrollo de las infraestructuras y las aplicaciones se requerían inversiones de capital elevadas. Para conseguirlo, se debían dar facilidades y, sobre todo, seguridades a las inversiones privadas. A su vez, se insistía en garantizar los derechos de los trabajadores en todos los sectores, garantizando mejoras mediante técnicas de trabajo a distancia, con sus distintas ventajas e inconvenientes.

Se debían poner a disposición de los ciudadanos todas aquellas mejoras que permitieran elevar su nivel de vida, conscientes de que los cambios sociales que se producían en los países industrializados eran el signo, en gran medida (aunque en absoluto de forma exclusiva), de una mutación hacia una sociedad postindustrial, caracterizada en particular por el papel central que en ella desempeñaría la información en todas sus formas, su producción, su difusión y su control.

Todo ello hizo intuir cambios tecnológicos profundos y avanzados, que darían lugar a grandes cambios sociológicos.

Un tema importante era garantizar que todos los ciudadanos tuvieran acceso a estas redes, tecnologías y servicios, estuvieran donde estuvieran, hecho que los monopolios trataron de conseguir mediante una política de ajuste tarifario, lo que provocó un problema eminentemente económico, ya que no toda la geografía de los estados miembros tenía un igual rendimiento. Este conjunto de situaciones requirió unas normativas y una jurisprudencia adecuadas a dicha realidad (29). Para ello se aplicó el concepto de servicio universal, para garantizar el suministro de las telecomunicaciones independiente de la localización del usuario, en el que el proceso de liberalización transformó un servicio público, en época de monopolio, en un servicio de interés general, en época de competencia.

El año 1994 es muy activo en cuanto a normativas (30), consultas y propuestas, introduciendo alternativas a las infraestructuras de los operadores incumbentes, mediante redes de televisión por cable (31) (32).

La resolución del Consejo (94/C 379/03) de 22 de diciembre de 1994 (33), relativa a los principios y al calendario de la liberalización de las infraestructuras de telecomunicaciones, planteó fechas concretas para la liberalización del suministro de infraestructuras de telecomunicaciones al 1 de enero de 1998, con un periodo transitorio de cinco años para aquellos estados miembros que lo requiriesen (España, Portugal, Grecia e Irlanda), y para las redes más pequeñas, si lo justificaban, de un plazo máximo de dos años.

Para llevar a cabo esta decisión, hubo que garantizar la elaboración del marco reglamentario imprescindible para asegurar la liberalización efectiva del suministro de infraestructuras de telecomunicaciones antes de esta fecha. Dicho marco reglamentario, incluidos los dispositivos de salvaguardia necesarios, instituiría principios comunes que garantizasen, mediante unos organismos reguladores de las telecomunicaciones, el suministro y la financiación de un servicio universal (34), normas en materia de interconexiones (25), determinación de condiciones y procedimientos de concesión de licencias (35), un acceso comparable y efectivo al mercado, una competencia leal, etc.

La evolución de las tecnologías digitales garantizó la convergencia de las comunicaciones tradicionales y nuevas, ya fuera utilizando imágenes, sonidos, datos y voz a través de redes diferentes. En esencia, uno de los factores más importantes fue el uso creciente de las mismas tecnologías en diferentes sectores, en particular en los de telecomunicaciones, medios de comunicación y tecnología de la información (TI) (36).

La evolución en ese momento del mercado parecía indicar que los operadores de los sectores afectados por la convergencia estaban intentando aprovechar las oportunidades que les ofrecía el progreso tecnológico para mejorar sus servicios tradicionales e irrumpir en actividades nuevas. En los sectores de las telecomunicaciones, los medios de comunicación y la tecnología de la información, se observó un desarrollo que no se detenía en las fronteras de los productos y las plataformas; todo lo contrario, se introdujeron en la adquisición de participaciones transectoriales.

Sin embargo, la convergencia no fue un concepto aplicable solamente a la tecnología, sino que significó también nuevos servicios y nuevas formas de actividad empresarial y de relación con la sociedad.

El carácter mundial de las plataformas de comunicación, y en particular de Internet, constituyó una llave que pudo abrir la puerta que conducía a una mayor integración de la economía mundial, lo cual supondría nuevas oportunidades y desafíos no solo para la Unión Europea, sino también para los estados de Europa central y oriental, los países mediterráneos y, en particular pensando en posibles ampliaciones, el mundo en vías de desarrollo. Por consiguiente, la globalización fue un aspecto clave de las tendencias futuras, a medida que las transformaciones que experimentó Europa se repitieran en otras partes del planeta.

También se instauró un marco que favoreció el mercado interior en materia de radiodifusión. Era imprescindible adaptar lo ya conseguido al marco reglamentario adecuado. Se esperaba que la aparición de servicios nuevos y el desarrollo de los ya existentes favoreciera la expansión del mercado de la información en general, proporcionando nuevas formas de acceso al ciudadano y potenciando el rico patrimonio cultural de Europa, su potencial innovador, y sus ambiciones creativas.

Otro aspecto a tener en cuenta fue la importancia política y económica del espectro radioeléctrico (37), columna que vertebra toda una serie de actividades industriales en sectores como las telecomunicaciones, la radiodifusión, los transportes, la I+D, o los servicios de interés general, y por ello reviste una considerable importancia económica, tanto por su valor de mercado como en términos de empleo. Habida cuenta de que muchos de los ámbitos mencionados fueron objeto de las correspondientes políticas comunitarias, la Comunidad

Europea tuvo un especial interés en el establecimiento de una política coherente en materia de espectro radioeléctrico.

Por más que su contribución directa a las actividades que nos ocupan sea variable, el espectro radioeléctrico constituye un recurso esencial cada vez más escaso. Aunque desde una perspectiva económica el valor del espectro puede determinarse en función del valor de los servicios cuya prestación hace posible, no es este un factor predominante que se suela tener en consideración en la gestión de dicho recurso.

Por entonces, ya se preveía la importancia que iba a tener el espectro en el desarrollo de la telefonía móvil, wifi y la televisión digital terrestre.

En el caso del Reino de España la Ley 32/1992, de 3 de diciembre, que modifica la Ley 31/1987 de Ordenación de las Telecomunicaciones; Ley 42/1995, de 22 de diciembre, de las Telecomunicaciones por Cable y la Ley 12/1997, de 24 de abril, de Liberalización de las Telecomunicaciones.

1.2. INTERNET, EL ORIGEN DE LA RED DE REDES. EL PARADIGMA DE INTERNET (38)

A lo largo de estos años, alrededor de medio siglo, "la red de redes" se convirtió en un activo irrenunciable para los ciudadanos, las empresas y las administraciones. En poco tiempo Internet se transformó en un instrumento que pasó de ser un experimento académico, a aportar a las economías desarrolladas unos 4,2 billones de dólares.

Internet surgió como solución a un enigma o problema original, a una encrucijada de los sectores de informática y las telecomunicaciones en la década de los setenta, ya que cada uno evolucionaba independientemente, al margen del otro.

El sector de informática estaba en pleno crecimiento gracias a los grandes equipos que daban servicio a empresas, universidades e instituciones. Los sistemas informáticos de la época se caracterizaban por utilizar *software* propietario, por lo que solían ser incompatibles con equipos de otro fabricante. Si se comunicaban con otras máquinas del mismo fabricante, debían adquirirse caras licencias correspondientes a los módulos de ambas máquinas.

En el mundo de las comunicaciones, predominaba aún el mundo de la voz y la conmutación de circuitos, con los monopolios estatales mencionados, quienes podían comercializar datos utilizando las técnicas de conmutación de circuitos, típicas de la telefonía, altamente ineficientes para la comunicación entre ordenadores, caracterizada no por un flujo constante de información, sino por un tráfico a ráfagas donde se alternan picos de transmisión con largos periodos de inactividad o silencio.

Como resultado, en esta época, el acceso a los recursos de computación era doblemente costoso, tanto por el coste de los supercomputadores, como por el coste de las conexiones hacia esos supercomputadores. Ese era el "enigma o problema original" ante el que se encontraba la comunidad científica.

La forma de hacer viable el acceso a los recursos de computación, era situar los supercomputadores en un lugar común y que fueran compartidos por muchos usuarios, conectándose a ellos de forma remota. Sin embargo, como hemos visto, conectarse al supercomputador a través de la red telefónica conmutada era también tremendamente caro.

De esta forma nació una búsqueda de métodos alternativos que permitiesen una conexión más asequible a los supercomputadores remotos. El paradigma era encontrar un sistema de comunicación entre ordenador, económico y eficiente.

De esa forma, la conmutación de paquetes y la multiplexación de varios flujos de información sobre el mismo medio físico resultaban más eficientes y satisfactorias para los usuarios, dado que, si los paquetes de datos se podían ir

intercalando, se evitaba que los grandes flujos de información copasen el canal.

Es en 1964 cuando diferentes estudios profundizan y trabajan en estos conceptos.

Una de las redes pioneras en aplicar estos novedosos conceptos, y quizá la más conocida, fue ARPAnet. Financiada por la Advanced Research Projects Agency (ARPA, Agencia de Proyectos de Investigación Avanzados de Defensa), dependiente del Departamento de Defensa de Estados Unidos, comenzó a diseñarse a finales de la década de los 60 (1967) con el objeto de demostrar la viabilidad de esta nueva tecnología de conmutación de paquetes, e impulsar la investigación nacional en este campo. Pese a que la financiación provino del ámbito militar, este proyecto siempre tuvo fines civiles, como lo demuestra el hecho de que siempre fue un proyecto público en vez de clasificado.

Fue a finales de 1971 cuando Ray Tomlinson, de forma altruista y por afición, creó un programa que permitía enviar correos electrónicos a otros usuarios de la red y estableció el símbolo @ como separador entre el nombre del usuario y el del ordenador.

En 1974, se produjo otro de los grandes hitos que daría lugar a lo que ya sí podremos denominar Internet: la publicación del protocolo TCP/IP por parte de Vinton Cerf y Robert Kahn. Este fue el resultado de un intenso trabajo que por fin daba respuesta al *Internetting problem*, es decir, a la interconexión de múltiples redes.

Tras la publicación del protocolo TCP/IP, ARPA encargó la aplicación inmediata del mismo a tres tipos de redes distintas. Esto permitió que en 1975 se hiciera la primera prueba de comunicación entre dos redes diferentes con el protocolo TCP/IP, y que en 1977 se interconectaran tres redes con tecnologías de acceso completamente distintas: ARPAnet, SATnet (red satelital) y PRnet (red radio terrestre).

1983 fue un año especialmente importante por otros tres acontecimientos.

- Se adaptó el código de TCP/IP y se incorporó de serie en los nuevos ordenadores basados en UNIX BSD.
- ARPAnet había mantenido desde su creación un sistema centralizado de nombres de dominio. Es decir, que los ordenadores que a ella se conectaban eran gestionados desde un único punto. No obstante, debido al gran crecimiento que se estaba viviendo, este sistema se tornaba inmanejable y es en 1983 cuando Paul Mockapetris publicó el sistema de nombres de dominio (DNS), un sistema escalable capaz de dar respuesta a este aumento en el número de ordenadores conectados.
- A finales de 1983 se produce una escisión de ARPAnet, MILnet, con el objetivo de proporcionar los servicios internos al sector de defensa.

De esta forma, ARPAnet se convierte de forma definitiva en una red civil, centrada únicamente en el apoyo al mundo académico y de la investigación.

La National Science Foundation net fue una red financiada, por la National Science Foundation (NSF, La Fundación Nacional de Ciencias, una agencia gubernamental de los Estados Unidos que impulsa investigación y educación fundamental en todos los campos no médicos de la Ciencia y la Ingeniería), ante la creciente demanda por parte de la academia de tener acceso a los recursos de supercomputación.

En 1984, la NSF lanzó un programa de supercomputación con el objetivo de hacerla accesible a toda la comunidad investigadora, no solo a los grupos reducidos de investigadores que en esas fechas podían permitirse la adquisición de estos equipos. No obstante, una parte fundamental para el éxito y la viabilidad del proyecto era desplegar una red que permitiese a todos sus usuarios acceder remotamente a los supercomputadores para que pudieran ser compartidos por un alto número de usuarios de manera eficiente. Rápidamente contó con interconexión a ARPAnet, lo que la erigió como red de gran valor. Además, debido a su carácter abierto, su uso se extendió rápidamente, interconectando las redes locales de campus universitarios y

reemplazando progresivamente a ARPAnet en estas funciones de red troncal.

Ello dio lugar a una inesperada demanda que provocó una gran cantidad de tráfico, obligando a aumentar su capacidad ya durante su primer año de actividad. La NSF pretendía con este objetivo involucrar al sector para generar una actividad comercial asociada a la red. De esta forma, la creación y mantenimiento de la NSFnet tenía como objetivo prestar servicios de forma subvencionada hasta que el interés comercial permitiera su sostenibilidad económica, momento en el cual el subsidio de la NSFnet dejaría de tener sentido.

1.2.1. El internet comercial

Fue a finales de los 80 cuando, dado el nivel de usuarios y su crecimiento, empiezan a surgir intereses comerciales. En la primera actualización de la NFSnet se pidió la colaboración del sector privado en los trabajos de mejora de la capacidad para que se generase el *know-how* que sería necesario en el futuro.

En 1988 comenzaron públicamente los debates sobre su posible privatización tras la aplicación de la "Directiva de uso aceptable" que prohibía utilizar la red troncal para otros usos que no estuviesen relacionados con la educación e investigación académica. Ese mismo año fue también cuando se publicó el informe "Towards a National Research Network" por el Consejo Nacional de Investigación. El informe suscitó el interés del entonces senador Al Gore quien lideró la puesta en marcha de la "National Information Infraestructure" a la que se refería como "las autopistas de la Información".

Mientras tanto, el uso de esta red continuaba creciendo a gran ritmo, lo que provocó que, tras el cierre de ARPAnet en 1990, se tuviese que abordar una nueva mejora de la red en 1991. En este mismo año ocurrió un hecho de vital importancia para el posterior crecimiento de Internet y su transición hacia una vertiente más doméstica y comercial: la aparición de la World Wide Web. Fue el 7 de agosto de 1991 cuando Tim Berners-Lee, investigador del CERN (Conseil Européen pour la Recherche Nucléaire), publicó un programa servidor y cliente, desarrollado en su tiempo libre, que marcó un antes y un después en la evolución de Internet, convirtiéndose en su interfaz de usuario predilecta:

- Espacio de información compartida mediante hiperenlaces URLs.
- Una interfaz de usuario que facilita el acceso a la información.

En 1994 Tim Berners-Lee funda el W3C (World Wide Web Consortium) en el MIT. En 1995, ya existían los suficientes intereses comerciales como para que las funciones de la NSFnet pudiesen ser asumidas por agentes privados y, por tanto, en 1995 se daba de baja a esta red.

En ese momento la red interconectaba a más de 100.000 redes públicas y privadas a lo largo del país, y fue sustituida por otras redes troncales operadas por agentes privados de acceso a Internet. Para ello se obligó a que todos los operadores que quisiesen prestar el servicio de red troncal que prestaba la NSFnet se tenían que interconectar obligatoriamente en al menos 4 puntos de acceso en los que debían intercambiar el tráfico de forma gratuita.

De esta forma, y pese a su privatización, se garantizaba que la red iba a continuar siendo abierta y se facilitaba la interconexión de nuevas redes. Este modelo de puntos de acceso donde intercambiar tráfico "entre iguales" ha sido replicado por todo el mundo como solución de facto para la interconexión de redes nacionales.

El surgimiento de Internet, inicialmente como una red para el uso académico y la experimentación, le ha conferido unas características que han marcado profundamente su desarrollo.

No se puede explicar la evolución de Internet y sus aplicaciones sin señalar que, desde el despliegue de las primeras redes de datos, estas fueran percibidas por la academia como una forma de crear y mantener un elevado grado

de autonomía frente a los Estados y las grandes empresas. Ni los Estados ni sus monopolios de telecomunicaciones favorecieron el surgimiento de estas redes.

La cultura del *software* libre o abierto ha sido una de las grandes fuerzas que han impulsado el crecimiento de Internet hasta la actualidad. Sirva de ejemplo que las tres tecnologías más importantes para su surgimiento y difusión (el protocolo TCP/IP, el servicio de correo electrónico y la Web) se publicaron gratuitamente.

Cuatro puntos se consideran los causantes de su éxito: el carácter abierto y global de Internet, la aparición de interfaces de usuarios intuitivas y amigables para el uso doméstico, y la conexión *best-effort* (mejor esfuerzo) extremo a extremo entre dos dispositivos. Internet surgió como un modo agnóstico de conexión ligado a sus características sociales del modelo de funcionamiento y de autogestión de la red.

Igualmente, el hecho de que Internet surgiese como la interconexión de múltiples redes de ámbito académico que operaban al margen del control de los gobiernos, permitió que **su gobernanza**, la gestión de sus recursos y su estandarización técnica se organizasen de una manera muy alejada de procesos formales. Por el contrario, esta gestión se realizaba de manera informal a través de grupos de trabajo donde sus miembros eran elegidos en función de su reputación académica y de sus contribuciones al desarrollo de la red.

De esta forma, el modelo de gobernanza basado en la contribución de las múltiples partes interesadas (modelo *multistakeholder*) ha permitido a Internet adaptarse con la suficiente rapidez a los cambios que han surgido durante estos años.

En quinto y último lugar, el proceso de privatización jugó un papel importante en el establecimiento de las bases de lo que ahora es Internet. La transición desde una red subvencionada hacia una red de agentes privados que se interconectan ha sido crucial para que esta red haya continuado creciendo y expandiéndose internacionalmente.

En el Reino de España Fundesco, una fundación de la Operadora Telefónica, era la encargada de suministrar el acceso de Internet a las Universidades y Centros de Investigación de manera altruista.

1.3. LA PRIMERA REVISIÓN. LA NORMALIZACIÓN EN EL PAQUETE DE DIRECTIVAS DE 2002, (1999-2005)

Una vez implantada la plena competencia en 1998, se inició el proceso de revisión del paquete de las directivas que se habían adoptado entre 1990 y 1997, con un objetivo doble.

En primer lugar, se trataba de revisar el alcance de las disposiciones adoptadas en la etapa anterior, a la luz de la experiencia del corto período transcurrido desde su implantación. Se pretendía aligerar, en la medida de lo posible, la intervención del Estado en el sector de las telecomunicaciones confiando en el paulatino y creciente buen funcionamiento de la competencia. Además, resultaba conveniente, desde el punto de vista jurídico, consolidar los textos del rosario de directivas por las que se había regulado el sector desde 1990.

En segundo lugar, se pretendía ampliar el alcance de la política de las Telecomunicaciones al terreno más general de las Comunicaciones electrónicas, permitiendo abordar aspectos relacionados con la convergencia tanto en lo que se refería a las infraestructuras como a la interoperabilidad de los servicios.

Esta etapa culminó con la adopción del paquete de directivas de 2002, y continuó con el largo proceso de su transposición a las legislaciones de los estados miembros, así como con el ajuste entre los Estados y la Comisión en los criterios para el análisis de los mercados, de acuerdo con el artículo 7 de la Directiva Marco.

Esta etapa coincidió plenamente con el planteamiento de la Estrategia de Lisboa y el

lanzamiento de la iniciativa eEurope, que trataría de integrar a las Comunicaciones electrónicas en la Política de la Unión Europea para el desarrollo de la Sociedad de la Información.

1.3.1. El modelo de competencia de servicios. Los operadores incumbentes

Hay que tener en cuenta algunos aspectos que se plantearon y se resolvieron respecto a la liberalización:

A) Reglamento sobre el Bucle local (39).

Tras la entrada en vigor de la plena competencia en 1998, se suponía que iba a traer una avalancha de inversiones en infraestructuras de telecomunicaciones; pero no fue así. Los nuevos operadores optaron por utilizar las infraestructuras de transmisión realizadas durante la época de los monopolios, en particular en lo referente a la última milla, es decir, el bucle local.

Posiblemente las expectativas generadas por la burbuja de Internet que ya era de considerable tamaño durante los primeros meses de 2000, contribuyeron a precipitar este episodio.

Ante las dudas de los operadores históricos, y para que las cosas quedaran claras, el mismo 24 de abril de 2000, la Comisión adoptó una comunicación específicamente dedicada al bucle local en la que se concluye que son de aplicación las normas de la competencia al acceso desglosado del bucle de abonado y que la negativa por parte de los operadores dominantes a abrirlo a los competidores podría considerarse como un abuso de su posición dominante.

Y a una velocidad inusitada, el Consejo y Parlamento adoptaron el **Reglamento relativo al bucle local**, que se publicó en el Diario oficial el 30 de diciembre del mismo año 2000, con lo que quedaron despejadas todas las dudas relativas a este asunto.

Se optó por los servicios en lugar de las infraestructuras. Había que dar respuesta a las necesidades que planteaban Internet y la sociedad de la información.

B) Directiva relativa a la competencia en los mercados de redes y servicios.

El 16 de septiembre de 2002, la Comisión adoptó la Directiva 2002/77 relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas, por la que se revalidaba el proceso de liberalización de las telecomunicaciones.

Hay que tener en cuenta que el artículo 86 (actual artículo 106) del Tratado, autoriza a la Comisión a adoptar directivas con objeto de garantizar que los servicios de interés general queden sometidos a las reglas de la competencia sin perjuicio de las misiones a ellos encomendadas.

La normativa europea estableció que los servicios de telecomunicaciones son servicios de interés general que se prestan en régimen de competencia. Solo tienen la consideración de servicio público o están sometidos a obligaciones de servicio público, los servicios de telecomunicaciones para la defensa nacional y la protección civil.

Con base en todo lo anterior, la Unión Europea comenzó a utilizar a partir de 2002 el término Política de Comunicaciones electrónicas, que englobaría lo referente a "las redes de comunicaciones electrónicas, a los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión", y como también queda aclarado, esta política no incluiría ni "los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos", ni tampoco "los servicios de la sociedad de la información".

Realmente se trataba de una Directiva que consolida y aclara el marco de la libre competencia en las redes y servicios de comunicaciones electrónicas que había ya quedado definido en 1998.

1.3.2. El paquete Telecom 2002

El proceso fue relativamente rápido. Como es habitual, la Comisión hizo un planteamiento que el Consejo y/o el Parlamento rechaza, matiza o acepta, sin olvidar los comentarios del Comité Económico y Social y del Comité de las Regiones. Y a partir de este resultado, se elaboró el documento (directiva, resolución...). Y posteriormente, claro está, la transposición en cada país.

El marco regulador de las comunicaciones electrónicas en Europa estaba constituido por 5 directivas básicas:

1. Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco): establece los principios generales, los objetivos del nuevo marco y los procedimientos básicos.
2. Directiva 2002/19/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de Acceso): establece los procedimientos para imponer obligaciones a los operadores con peso significativo en el mercado (PSM).
3. Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de Autorización): establece el sistema de títulos habilitantes bajo el principio de mínima intervención.
4. Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva de Servicio Universal).
5. Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

En estas directivas se definen y aclaran aspectos tales como la función de las autoridades nacionales de reglamentación, se introduce una simple autorización general para el suministro de redes y servicios, se recoge aspectos específicos con relación a la desagregación y el acceso al bucle de abonado, las obligaciones del servicio universal y la salvaguardia de la intimidad de los usuarios de los servicios de comunicaciones electrónicas, etc.

La transposición de estas directivas dio lugar a leyes específicas en los estados miembros (Ley General de Telecomunicaciones 03/11/2003; Ley de Servicios de la Sociedad de la Información y Comercio Electrónico 11/07/2002; en el caso español).

El conflictivo tema de la comunicación audiovisual se retrasó hasta la Directiva 2007/65/CE, (Ley 07/2010 de 31/03/2010, General de la Comunicación Audiovisual, en el caso español).

1.4. LA SEGUNDA REVISIÓN (2005-2010)

De acuerdo con otros autores, vamos a ver los aspectos estratégicos de la revisión de 2005-2010 (40) (41).

Tal como indicaban las directivas del paquete de 2002, durante 2005 la Comisión debía informar acerca de la evolución del marco regulador de las comunicaciones electrónicas, y así lo hizo. La Comisión Barroso, que había iniciado sus actividades a finales de 2004, ejecutó el mandato en el contexto de sus nuevos objetivos.

Hay que señalar que en la nueva estructura del ejecutivo comunitario se unificaron las responsabilidades de la Política de la Sociedad de la Información y de la Política Audiovisual y Medios. Esta medida iba a garantizar la

adopción de planteamientos convergentes en ambas políticas.

El nuevo proceso de revisión iba a girar en torno a dos ejes fundamentales: el primero, la actualización de la política, ya tradicional, de comunicaciones electrónicas; y el segundo, el intento de búsqueda de soluciones reglamentarias a los nuevos servicios audiovisuales.

La declaración de principios de lo que iba a ser la futura política impulsada por la Comisión quedó definida en la iniciativa i2010 para el desarrollo de la sociedad de la información (42).

A partir de la entrada en vigor de la libre competencia en este sector, la Política de Comunicaciones electrónicas de la Unión Europea pasó a formar parte de su Política para el desarrollo de la Sociedad de la Información.

En resumen, en el apartado del espacio único europeo de la información, la iniciativa i2010 aceleró la obtención de dividendos económicos de la convergencia digital a través de las medidas siguientes: revisar el marco regulador de las comunicaciones electrónicas (2006) definiendo en particular una estrategia para la gestión eficiente del espectro (2005); y crear un marco coherente para el mercado interior de los servicios de la sociedad de la información y los medios de comunicación.

De acuerdo con dicho planteamiento, la Comisión puso en marcha, por una parte, el proceso de revisión del marco regulador de las comunicaciones electrónicas, y por otra, reactivó las actuaciones que venía llevando a cabo en el sector audiovisual.

1.4.1. El paquete Telecom 2009

La Comisión publicó en noviembre de 2005 un documento preparatorio para solicitar la opinión de las partes interesadas del sector. De forma ilustrativa vamos a exponer el proceso que llevó a la reforma de la Política de Comunicaciones electrónicas en la Unión Europea.

En 2007, casi un año después del cierre de la consulta pública, la Comisión publicaba una comunicación para informar sobre los resultados de la revisión y para explicar las principales modificaciones propuestas por la Comisión para el marco regulador. Tales propuestas pasaron a denominarse "las propuestas de reforma de 2007".

Los detalles de las propuestas legislativas de la Comisión estaban contenidos en tres comunicaciones y en la correspondiente evaluación de impacto.

Dos de las comunicaciones contenían sendas propuestas de modificación de las directivas específicas de 2002; concretamente una propuesta de modificación de las Directivas Marco/Autorización/Acceso y una propuesta de modificación de la Directiva de Servicio Universal.

La tercera comunicación, por su parte, contenía una propuesta de reglamento para la creación de la Autoridad del Mercado de las Comunicaciones Electrónicas (EECMA, *European Electronic Communications Market Authority*).

La Comisión enumeraba los resultados y los agrupaba en tres grupos, cada uno correspondiente a una propuesta de directiva o reglamento:

- Legislar mejor para conseguir unas comunicaciones electrónicas competitivas, donde incluía la simplificación de la regulación y la nueva legislación sobre espectro radioeléctrico: interoperabilidad de los servicios inalámbricos en toda la UE, uso del dividendo digital y cualquier frecuencia para cualquier aplicación, aunque garantizando el pluralismo de los medios de comunicación.
- Conectar con los ciudadanos, donde se incluyeron las propuestas relativas:
    1. A la protección de los consumidores, tales como mejorar la transparencia de la información facilitada por los operadores o permitir que las Autoridades Nacionales de Reglamentación (ANR) impusiesen unos requisitos mínimos de calidad de los servicios.

2. A la accesibilidad electrónica.
3. Al refuerzo de la seguridad de las redes y los servicios, así como la privacidad de los usuarios.

Ya, con un procedimiento de codirección el nuevo marco regulador, quedó definitivamente aprobado el 25/11/2009 mediante las directivas:

1. *Better Regulation* (en adelante, "Legislar mejor").
2. *Citizens' Rights* (en adelante, "Derechos de los ciudadanos") y el Reglamento de creación del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (BEREC, *Body of European Regulators for Electronic Communications*).

Recomendamos ver la Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº2006/2004 sobre la cooperación en materia de protección de los consumidores (Directiva Derechos de los Usuarios).

Igualmente, recomendamos ver la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CE, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE, de 7 de marzo de 2002, del Parlamento Europeo y del Consejo, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión y la Directiva 2002/20/CE, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva Mejor Regulación).

Sigue vigente la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

En el Reino de España estas directivas fueron transpuestas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

1.4.2. Sector audiovisual

De las primeras acciones de CEE en materia de medios audiovisuales, cuando los medios técnicos para la difusión de televisión (en particular el cable y el satélite) permitieron que estas emisiones superaran las fronteras de los países la Comunidad Europea, fue la llamada Directiva Televisión sin fronteras (43) por la que se ordenaba a los estados miembros que se abstuvieran de obstaculizar la retransmisión en sus territorios de emisiones procedentes de otros estados miembros.

La digitalización de las redes, la liberalización de las infraestructuras, y las posibilidades de prestación de distintos tipos de servicios a través de las mismas, obligaron a la Comisión ya en 1999 (44) a adoptar una nueva directiva que modificaba una vez más a la Directiva 90/388 (45), con objeto de ordenar la separación de los negocios de telecomunicaciones y televisión, y lo hacía en los términos siguientes:

"Los estados miembros velarán por que ningún organismo de telecomunicaciones explote su red de televisión por cable por medio de la misma entidad jurídica utilizada para su red pública de telecomunicaciones cuando tales organismos:

a) estén bajo el control del estado miembro de que se trate o goce de derechos especiales,
b) ocupe una posición dominante en una parte sustancial del mercado común de suministro de redes públicas de telecomunicaciones y servicios públicos de telefonía vocal, y
c) exploten, en la misma zona geográfica, una red de televisión por cable con arreglo a unos derechos especiales o exclusivos."

Con esta Directiva quedaba cerrado el proceso de liberalización en vísperas del inicio de la revisión del marco reglamentario del sector.

Es de destacar el sistemático intento de separar telecomunicaciones y medios de comunicación, independientemente que soporte utilice este último.

Propuestas, consultas y estudios sucedieron al Informe de la Comisión en lo que vino a llamarse proceso de modernización de la Directiva televisión sin fronteras, hasta que en 2005 la Comisión presentó al Parlamento y al Consejo su propuesta de Directiva para modificar, por segunda vez, la Directiva 89/552. La propuesta había estado trabajándose como televisión sin fronteras, pero se pasó a llamar Directiva de "servicios de medios audiovisuales".

Hay que decir que este cambio de denominación no fue casual y que la denominación "servicios de medios audiovisuales" era la que sustituiría a la de "emisiones de radiodifusión televisiva", que venía figurando en la Directiva. Definitivamente los problemas de la televisión sin fronteras habían dejado de serlo.

Contrario a lo dicho anteriormente, en este documento aparecen menciones a la nueva iniciativa i2010 y a la convergencia, como no podía ser menos, después de, como ya se ha dicho, que ambas Políticas, Sociedad de la Información y Medios Audiovisuales, hubiesen sido puestas bajo la responsabilidad del mismo miembro de la Comisión.

Del texto de la propuesta de Directiva conviene destacar la definición dada de los servicios de medios audiovisuales: "un servicio, tal como lo definen los artículos 49 y 50 [actuales 56 y 57] del Tratado, cuya principal finalidad es proporcionar imágenes en movimiento, acompañadas o no de sonido, con objeto de informar, entretener o educar al público en general, a través de redes de comunicaciones electrónicas, tal como las define la letra a) del artículo 2 de la Directiva 2002/21/CE del Parlamento y del Consejo".

Está claro que la futura Directiva de servicios de medios audiovisuales permitiría aplicar los principios básicos de la televisión a todas las nuevas formas de difusión de la Sociedad de la Información.

De acuerdo con lo anterior había que dejar claro cuál era el alcance de la pretendida convergencia. Según la propuesta de Directiva, y el texto de la Directiva finalmente adoptada, los servicios de medios audiovisuales, cualquiera que sea la red por la que se transmitan, continuarían sometidos al régimen jurídico que hasta entonces había regido para la televisión. Así las cosas, la única convergencia que ha permanecido es la relativa a las redes de comunicaciones electrónicas en vigor desde 1998.

El proceso de codecisión se prolongó hasta noviembre de 2007, cuando el Parlamento adoptó la Directiva después de que el Consejo adoptase una Posición Común en mayo de 2007. La nueva Directiva entró en vigor el 19 de diciembre de 2007. En febrero de 2010, el Consejo adoptó una versión codificada. Respecto de la denominación, cabe decir que la Directiva adoptó finalmente la de "servicios de comunicación audiovisual" (46).

La Directiva de servicios de comunicación audiovisual de UE, 2010, (47) pretendía crear y garantizar el funcionamiento adecuado de un mercado de servicios de comunicación audiovisual en la Unión Europea, al tiempo que contribuía a la promoción de la diversidad cultural y ofrecer un nivel adecuado de protección del consumidor y del menor. A su vez, regía la coordinación en todo el territorio de la UE de la legislación nacional sobre toda la comunicación audiovisual, tanto las emisiones televisivas tradicionales como los servicios de comunicación audiovisual a petición.

Los prestadores de servicio de intercambio de vídeos a través de plataforma tenían las mismas obligaciones que los prestadores de servicios de comunicación respecto a la publicidad y otras restricciones de contenido, teniendo en cuenta el control limitado que pueden ejercer sobre la publicidad en sus plataformas que no es comercializada, vendida u organizada por ellos.

Hubo que esperar a 2014 para la creación del Grupo de Reguladores Europeos de Servicios de Medios Audiovisuales (ERGA), que reúne a jefes

y representantes de alto nivel de organismos reguladores nacionales independientes en el ámbito de los servicios audiovisuales. Estos representantes asesoran a la Comisión sobre la aplicación de la DSCA.

La Directiva (UE) 2018/1808 (48) modifica y actualiza la Directiva de servicios de comunicación audiovisual, como parte de la Estrategia para el Mercado Único Digital.

La revisión de la DSCA en 2018 reforzó el papel de ERGA (Grupo de Entidades Reguladoras Europeas de los Servicios de Comunicación Audiovisual, creada en 2014), introduciendo requisitos específicos para garantizar la independencia de las autoridades nacionales de reglamentación.

Esta directiva se traspone al caso del Reino de España mediante la Ley 13/2022, 7 de julio, General de Comunicación Audiovisual.

1.5. NUEVOS ASPECTOS DE LA POLÍTICA DE TELECOMUNICACIONES. REDES DE MUY ALTA CAPACIDAD (2010-2024)

La economía mundial se está convirtiendo rápidamente en digital (49). Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico, sino el fundamento de todos los sistemas económicos innovadores modernos. Internet y las tecnologías digitales están transformando la vida que llevamos y la forma en que trabajamos (como personas, en las empresas y en nuestras comunidades) cuanto más se integran en todos los sectores de nuestra economía y nuestra sociedad.

Estos cambios se suceden a una escala y una velocidad que ofrecen inmensas oportunidades para la innovación, el crecimiento y el empleo. También plantean difíciles cuestiones políticas a las autoridades públicas, lo que exige una acción coordinada de la UE. Todos los estados miembros se enfrentan a problemas similares, pero sobre una base nacional, lo que supone una limitación para aprovechar todas las oportunidades y afrontar todos los retos de esta transformación. En numerosos ámbitos, el nivel europeo es el marco adecuado. Por esta razón, la Comisión Europea ha fijado como una de sus principales prioridades la creación de un mercado único digital.

Recordemos que un mercado único digital es aquél en el que la libre circulación de mercancías, personas, servicios y capitales está garantizada, y en el que personas y empresas pueden acceder fácilmente a las actividades y ejercerlas en línea en condiciones de competencia, con un alto nivel de protección de los datos personales y de los consumidores, con independencia de su nacionalidad o lugar de residencia. Lograr un mercado único digital permitirá que Europa mantenga su posición de líder mundial en la economía digital, lo que ayudará a las empresas europeas a crecer a escala mundial.

Europa tiene capacidad de liderazgo en la economía digital mundial, pero actualmente no le está sacando el máximo partido. La fragmentación y las barreras, que no existen en el mercado único físico, frena a la UE. Reducir estas barreras dentro de Europa podría aportar un importe adicional de 415.000 millones EUR al PIB europeo. La economía digital puede ampliar mercados y promover mejores servicios a mejores precios, ofrecer mayores posibilidades de elección y crear nuevas fuentes de empleo. Un mercado único digital puede crear oportunidades para las empresas emergentes y permitir que las empresas existentes crezcan y se beneficien de la escala de un mercado de más de 450 millones de personas, de momento.

Para conseguirlo, la UE plantea una estrategia basada en tres pilares:

- Mejorar el acceso de los consumidores y las empresas a los bienes y servicios en línea en toda Europa: lo que exigirá que se eliminen rápidamente las diferencias fundamentales entre los mundos en línea y fuera de línea, para derribar las barreras a la actividad transfronteriza en línea.

- Crear las condiciones adecuadas para que las redes y servicios digitales prosperen: lo que requiere infraestructuras de alta velocidad y servicios de contenidos seguros y fiables, apoyados por unas condiciones reguladoras correctas que favorezcan la innovación, la inversión, la competencia leal y la igualdad de condiciones.
- Aprovechar al máximo el potencial de crecimiento de nuestra economía digital europea: lo que requiere una inversión en infraestructuras de las TIC y tecnologías como la computación en nube y los datos masivos, e investigación e innovación para impulsar la competitividad industrial, así como la mejora de los servicios públicos, la inclusividad y las cualificaciones.

Muchos deben ser los cambios a introducir en la Política de Telecomunicaciones y Sociedad de la Información, que Jean-Claude Juncker resumió en un párrafo de sus directrices políticas al acceder al cargo de presidente de la Comisión Europea:

"Creo que debemos utilizar mucho mejor las grandes oportunidades que ofrecen las tecnologías digitales, que no conocen fronteras. Para ello, necesitamos tener el valor de abrir los compartimentos nacionales de regulación de las telecomunicaciones, de derechos de propiedad intelectual y de legislación sobre protección de datos".

En el caso del Reino de España estas directivas, se transponen en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

1.5.1. Código europeo de las comunicaciones electrónicas

Una acción importante es la publicación de la directiva 2018/1972 (50) conocida como el Código Europeo de Comunicaciones Electrónicas, que, según la propia UE:

- establece una serie de normas actualizadas para regular las redes de comunicaciones electrónicas (telecomunicaciones), los servicios de telecomunicaciones, así como los recursos y servicios asociados;
- presenta tareas para las autoridades nacionales de reglamentación y otras autoridades competentes, y establece una serie de procedimientos para garantizar la armonización del marco regulador en toda Europa;
- pretende estimular la competencia y aumentar la inversión en 5G y en redes de muy alta capacidad, para que todos los ciudadanos y las empresas de la UE puedan disfrutar de una conectividad de alto nivel, un elevado nivel de protección del consumidor y una mayor variedad de servicios digitales innovadores.

A nuestro entender, sus puntos clave son:

- La Directiva establece un Código Europeo de las Comunicaciones Electrónicas, un conjunto amplio de normas nuevas o revisadas para el sector de las telecomunicaciones como parte de un paquete de leyes sobre telecomunicaciones, incluido el Reglamento (UE) 2018/1971 (51) por el que se establecen el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Agencia de apoyo al ORECE (Oficina del ORECE).
- Sustituye y deroga las Directivas 2002/19/CE (52), 2002/20/CE (53) y 2002/21/CE (54), así como el artículo 5 de la Decisión n.° 243/2012/UE (competencia en espectro) (55). La revisión de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) (57) se lleva a cabo por separado (58).
- Promueve la conectividad y la adopción de redes de muy alta capacidad, incluidas las redes fijas, móviles e inalámbricas, para todos los ciudadanos y empresas de la UE.
- Promueve los intereses de los ciudadanos de la UE:
  - — Permitiendo maximizar los beneficios en cuanto a variedad de elección, precio y calidad a través de una competencia efectiva.
  - — Manteniendo la seguridad de la red y los servicios.

— Garantizando la protección de los consumidores a través de normas específicas.

— Abordando las necesidades de grupos sociales específicos, en particular las personas con discapacidad, las personas mayores y las personas con necesidades sociales especiales.

- Facilita la entrada en el mercado y promover la competencia en el suministro de redes de telecomunicaciones y recursos asociados.
- Contribuye al desarrollo del mercado interno en las redes y servicios de telecomunicaciones de la UE, desarrollando normas comunes y una normativa predecible caracterizada por:

  — El uso efectivo, eficiente y coordinado del espectro radioeléctrico.

  — La innovación abierta.

  — El desarrollo de redes transeuropeas.

  — La disponibilidad e interoperabilidad de servicios paneuropeos.

  — La conectividad de extremo a extremo.

Además de sustituir y derogar la legislación existente, la Directiva introduce una serie de nuevos objetivos y funciones:

- Normas acerca de los consumidores más estrictas, con el objetivo de facilitar el cambio entre proveedores de servicio y ofrecer una mejor protección, por ejemplo, a las personas que se abonan a servicios empaquetados. Los consumidores se beneficiarán de un mayor nivel de protección similar en toda la UE.
- Actualmente, los servicios de telecomunicaciones incluyen servicios ofrecidos por internet que no utilizan números de teléfono, como aplicaciones de mensajería y correo electrónico. Un mecanismo de revisión pretende garantizar que los derechos de los consumidores sigan siendo sólidos y sigan estando actualizados a medida que los modelos de negocio y el comportamiento de los consumidores cambian.
- El acceso adecuado a una internet de banda ancha asequible debe estar disponible para todos los consumidores, con independencia de su ubicación o renta, servicio universal.
- Las personas con discapacidad deben tener un acceso equivalente a los servicios de telecomunicaciones.
- Los países de la UE crearán un sistema de alerta al público para enviar alertas a los teléfonos móviles de los ciudadanos en caso de catástrofe natural u otra emergencia grave en su zona.
- Los países de la UE deben ofrecer a los operadores una normativa predecible para la concesión de licencias relativas al espectro radioeléctrico para banda ancha inalámbrica durante al menos 20 años con el fin de promover la inversión, en particular en conectividad 5G. Asimismo, se persigue un aumento de la convergencia de los procedimientos nacionales de selección a través de un foro de revisión por pares.
- Nuevas bandas de frecuencia (dividendo digital) para la conectividad 5G para conexiones a internet más rápidas y una mejor conectividad, así como coordinación temporal de la concesión de licencias relativas al espectro y un régimen reglamentario menos estricto para el despliegue de pequeños componentes de equipos de redes móviles.
- Las normas sobre el acceso de los operadores a las redes para fomentar la competencia facilitan la inversión de las empresas en nuevas infraestructuras de muy alta capacidad (velocidades de descarga de 100 Mbps o más, nueva generación de redes), también en zonas remotas, al tiempo que garantizan una regulación efectiva del mercado.
- Las nuevas herramientas abordarán problemas que pueden surgir en ciertas circunstancias del mercado. Se aplicará una reglamentación simétrica (misma reglamentación para todos los proveedores de red) a todos los proveedores de redes de comunicaciones electrónicas en ciertas situaciones muy específicas para garantizar la competencia.

1.5.2. El organismo de reguladores europeos de las comunicaciones electrónicas

Conviene recordar que por política para las comunicaciones electrónicas entendemos el conjunto de actuaciones de carácter estratégico, reglamentario y, en menor medida, presupuestario adoptadas por las instituciones comunitarias con el objeto de conseguir los objetivos de la Unión Europea a través de esta área de actividad.

A su vez, la política de comunicaciones electrónicas suele presentarse como el resultado de la progresiva convergencia tecnológica de las telecomunicaciones, los medios de comunicación y las tecnologías de la información. La Unión Europea la considera como parte integrante de su Política para el Desarrollo de la Sociedad de la Información.

Y es en este contexto en el que hay que ubicar el marco regulatorio de las comunicaciones electrónicas que entenderemos constituido por las disposiciones de carácter legal adoptadas por las instituciones europeas, que posteriormente serán transpuestas a las legislaciones de los estados miembros y cuyo objetivo es el de regular la explotación de los servicios y las redes de comunicaciones electrónicas en el marco de la libre competencia así como establecer los derechos básicos de los ciudadanos en estas materias.

Esta política deberá contemplar forzosamente los tres planos socioeconómicos en los que tiene incidencia este sector. En primer lugar, el plano macroeconómico, de interés para el conjunto de la Unión Europea y de sus estados miembros; en segundo lugar, el plano microeconómico, de interés para las empresas que conforman el sector; y, en tercer lugar, el plano individual, que afecta a todos y a cada uno de los ciudadanos en su condición de usuarios de los servicios de las comunicaciones electrónicas.

Por estos motivos la política de las comunicaciones electrónicas de la Unión Europea ha tenido y continuará teniendo un carácter subsidiario de las políticas en los estados miembros en este sector debido a la imposibilidad de definir, desde instancias comunitarias, una estrategia completa y coherente común a toda la Unión que abarque en su conjunto los aspectos macroeconómicos, microeconómicos e individuales.

Pero ello no es óbice para que el Tratado de Funcionamiento de la Unión Europea conceda a las instituciones europeas competencias suficientes para abordar la elaboración de una política de comunicaciones electrónicas y, fundamentalmente, un marco regulatorio común que contribuya a la creación del mercado interior en este sector.

En 2018, mediante el Reglamento 2018/1971 (51), se consolida la regulación tendente a crear un mercado interior de las comunicaciones electrónicas (ORECE) asignándole un número importante de nuevos cometidos, como la formulación de directrices en diversos ámbitos, la presentación de informes sobre cuestiones técnicas, el mantenimiento de registros, listas o bases de datos y la elaboración de dictámenes sobre procedimientos del mercado interior para proyectos de medidas nacionales relativas a la regulación del mercado, actuando o eliminando anteriores reglamentos y reforzando el Código Europeo de las Comunicaciones Electrónicas.

El ORECE (BEREC en inglés) y su oficina, creados en 2009 (59), con sede en Riga, han contribuido al buen funcionamiento de las comunicaciones electrónicas en el marco conjunto de la UE, por ejemplo, en la itinerancia en este marco, el acceso a una Internet abierta y libre, neutralidad de la red europea, etc.

En su momento sustituye al grupo de entidades reguladoras europeas de las redes y servicios de comunicaciones electrónicas (GRE), dándole un aspecto más global. Sirviendo asimismo de órgano de reflexión, debate y asesoramiento en el ámbito de las comunicaciones electrónicas para el Parlamento Europeo, el Consejo y la Comisión.

En su comunicación del 6 de mayo de 2015 titulada “Una estrategia para el mercado único digital de Europa” (60), la Comisión preveía presentar propuestas en 2016 para

una revisión ambiciosa del marco regulador de las comunicaciones electrónicas centrada, entre otros aspectos, en un marco regulador institucional más eficaz a fin de adaptar la normativa de comunicaciones electrónicas a los fines previstos en el marco de la creación de las condiciones apropiadas para el mercado único digital.

No obstante, sigue habiendo importantes disparidades entre los estados miembros en lo que se refiere a las prácticas reguladoras, lo que afecta a las empresas que realizan negocios transfronterizos o que están activas en un número importante de estados miembros, en particular en aquellas zonas en las que las directrices del ORECE existen, pero podrían desarrollarse en mayor medida.

A la luz de la evolución de la tecnología y del mercado, que a menudo conlleva una mayor dimensión transfronteriza, y de la experiencia adquirida hasta la fecha a la hora de intentar garantizar la aplicación coherente en el ámbito de las comunicaciones electrónicas, es necesario basarse en los trabajos del ORECE y de la Oficina. Su gobernanza y actividades deben ser sencillas y adecuadas para desempeñar los cometidos que les hayan sido encomendados.

A la luz de la convergencia creciente entre los sectores proveedores de servicios de comunicaciones electrónicas, y de la dimensión horizontal de las cuestiones reglamentarias relacionadas con su desarrollo, el ORECE y la Oficina del ORECE deben poder cooperar, sin perjuicio del papel que desempeñen, con las autoridades nacionales de reglamentación, otros organismos, oficinas, agencias y grupos consultivos de la Unión, en particular el Grupo de política del espectro radioeléctrico, creado por la Decisión 2002/622/CE (61) de la Comisión, el Supervisor Europeo de Protección de Datos, establecido por el Reglamento (UE) 2018/1725 (62) del Parlamento Europeo y del Consejo, el Comité Europeo de Protección de Datos establecido por el Reglamento (UE) 2016/679 (63) del Parlamento Europeo y del Consejo, el Grupo de entidades reguladoras europeas para los servicios de comunicación audiovisual, establecido por la Directiva 2010/13/UE (64) del Parlamento Europeo y del Consejo, la Agencia de Seguridad de las Redes de la Información de la Unión Europea, creada por el Reglamento (UE) n.° 526/2013 (65) del Parlamento Europeo y del Consejo, la Agencia del GNSS Europeo creada por el Reglamento (UE) n.° 912/2010 (66) del Parlamento Europeo y del Consejo, la Red de Cooperación para la Protección de los Consumidores, creada en virtud del Reglamento (CE) n.° 2006/2004 (67) del Parlamento Europeo y del Consejo, la Red Europea de Competencia y organizaciones europeas de normalización, así como con los comités existentes (como el Comité de Comunicaciones y el Comité del Espectro Radioeléctrico).

El ORECE y la Oficina del ORECE también deben ser capaces de cooperar con las autoridades competentes de los estados miembros responsables de la competencia, la protección de los consumidores y la protección de datos, y con las autoridades competentes de terceros países, en particular con las autoridades reguladoras competentes en el ámbito de las comunicaciones electrónicas o con grupos de esas autoridades, así como con organizaciones internacionales cuando sea necesario para el desempeño de sus cometidos. El ORECE debe igualmente poder consultar a las partes interesadas mediante consulta pública.

1.5.3. La política del espectro radioeléctrico. Telefonía móvil. Reparto del espectro

El espectro radioeléctrico es un recurso natural de carácter limitado, sobre un bien público que gestiona el Estado. Esto quiere decir que, al ser un recurso natural, no se puede crear, es decir, nos lo proporciona de forma natural nuestro planeta, por eso es público, pero tiene la potestad de su uso el gobierno del país sobre el que está.

El espectro radioeléctrico es intangible y puede usarse por diferentes servicios de telecomunicación, por ejemplo, internet, telefonía, televisión,

radio. El espectro radioeléctrico está compuesto por una serie de frecuencias, conocidas como "banda de frecuencias", que solo pueden utilizar legalmente los que tengan una licencia (título habilitante) de telecomunicaciones, o quien la disponga se la ceda a un tercero o también personal autorizado como, por ejemplo, para usarlo en servicios como defensa, seguridad, emergencias, transportistas, radioaficionados o investigaciones científicas, siempre y cuando tengan su debida autorización.

Hay bandas de frecuencias que son libres, es decir, no es necesario una licencia, como por ejemplo ocurre con el wifi cuando utiliza las bandas de 2.4 GHz y 5 GHz.

En la actualidad, la mayor demanda del espectro radioeléctrico recae sobre todo en los servicios inalámbricos de telefonía, televisión o internet por 3G, 4G, y el actual 5G.

Históricamente ha sido necesario llegar a acuerdos en la distribución geográfica de las radiofrecuencias, y para ello se han creado organizaciones e instituciones que han dado lugar a convenios internaciones país a país, o en nuestro caso con la UE, siendo la más importante la Unión Internacional de Telecomunicaciones (UIT). Periódicamente se reúne la UIT en Conferencia Mundial de Radiocomunicaciones, donde se actualiza, se debate y se atiende las necesidades del sector.

El Marco regulador de 2002 consiguió abarcar la política de la UE en materia del espectro radioeléctrico mediante la aprobación de la Decisión Espectro Radioeléctrico (DER) en marzo de 2002 (68).

La DER establecía procedimientos con objeto de:

- Facilitar el proceso de decisión con respecto a planificación estratégica y la armonización del uso del espectro radioeléctrico en la Comunidad.
- Velar por la aplicación eficaz de la política del espectro radioeléctrico en la Comunidad.
- Garantizar la publicación, rápida y coordinada, de información sobre la atribución, disponibilidad y uso del espectro radioeléctrico en la Comunidad, como por ejemplo los cuadros nacionales de atribución de frecuencias o las tasas y cánones relativos al uso del espectro.
- Velar por la coordinación efectiva de los intereses de la Comunidad en las negociaciones internacionales, como por ejemplo las correspondientes a las Conferencias Mundiales de Radiocomunicación de la UIT.

La DER se basaba en el principio de que, cuando el Parlamento Europeo y el Consejo hubiesen llegado a un acuerdo sobre una política comunitaria en materia de espectro radioeléctrico, se debía recurrir a procedimientos de comitología (La Comitología en la Unión Europea refiere a un proceso mediante el cual se modifica y/o ajusta la legislación de la UE, llevando esto a cabo dentro de los "comités de comitología" presididos por la Comisión Europea. El término oficial para este proceso es procedimiento de comité para la adopción de las medidas técnicas de aplicación que lo acompañasen (considerando 4). Y como contrapartida, cuando fuese necesario adoptar medidas de armonización para la aplicación de políticas comunitarias que fuesen más allá de las medidas técnicas de aplicación, la Comisión presentaría al Parlamento Europeo y al Consejo una propuesta basada en el Tratado (considerando 7).

El procedimiento de comitología se implementó mediante la creación del Comité del espectro radioeléctrico (RSC, *Radio Spectrum Committee*), para asistir a la Comisión. Compuesto por representantes de los estados miembros y presidido por un representante de la Comisión.

Por su parte, la Comisión creó el Grupo de Política del Espectro Radioeléctrico (RSPG). Se trataba de un órgano consultivo, *sui géneris*, encargado de asistir y asesorar a la Comisión sobre temas de alcance político más amplio que las medidas técnicas habitualmente abordadas por el Comité RSC.

Con la decisión de 2012 (69), se establece un programa plurianual de política del espectro radioeléctrico en toda la UE para contribuir a la planificación estratégica de su uso en todas las políticas de la UE relacionadas con el mercado interior, como las comunicaciones electrónicas,

la banda ancha inalámbrica, las comunicaciones móviles y el internet de las cosas (IdC), el transporte, la energía y los medios audiovisuales.

Se está flexibilizando la utilización del espectro, sin dejar su control, para disponer de una cobertura y capacidad suficientes para alcanzar las mayores velocidades de banda ancha inalámbrica.

La directiva que establece el Código Europeo de las Comunicaciones Electrónicas introduciendo normas sobre la coordinación del espectro radioeléctrico entre los países de la UE y armoniza las normas para su gestión, incluye normas específicas para facilitar la entrada en el mercado a los nuevos actores y para el uso compartido del espectro radioeléctrico. Pretende estimular la competencia y aumentar la inversión en 5G y en redes de muy alta capacidad, para que todos los ciudadanos y las empresas de la UE puedan disfrutar de una conectividad de alto nivel, un elevado nivel de protección del consumidor y una mayor variedad de servicios digitales innovadores.

1.5.3.1. Principales usos del espectro radioeléctrico en comunicaciones electrónicas

Precisando, la decisión de la Comisión de 2019 (70) constituye el Grupo de política del espectro radioeléctrico (RSPG) un grupo consultivo de alto nivel, compuesto por autoridades de cada uno de los estados miembros que se ha creado para ayudar a la Comisión Europea (71) a formular la política del espectro radioeléctrico. Teniendo en cuenta consideraciones técnicas, económicas, políticas, culturales, estratégicas, sanitarias y sociales, junto con las necesidades potencialmente encontradas de los usuarios del espectro radioeléctrico, y tiene por objeto velar por que se logre un equilibrio justo, no discriminatorio y proporcionado.

El uso eficiente del espectro radioeléctrico, de cara a un mercado único europeo, requería en primera instancia el paso de la televisión analógica a la digital cuyas ventajas son similares a las de otros medios de transmisión digital en plataformas tales como la televisión por cable y televisión por satélite: capacidad de transmisión de audio y vídeo de mejor calidad y menores costes de transmisión, después de los costes de actualización.

El espacio antes empleado por una sola señal de televisión, mediante el canal múltiple digital, ahora serán varias las señales emitidas por dicho canal, y el espectro sobrante se puede utilizar para otros servicios, por ejemplo, internet. Resumiendo, las ventajas de la televisión digital frente a la analógica son más canales, mejor calidad de imagen y sonido y más servicios (dividendo digital).

1.5.3.1.1. Comunicaciones vía satélite

Las comunicaciones vía satélite usan del espectro radioeléctrico por lo cual la UE ha tratado de sacar la máxima rentabilidad digitalizándolas y ampliando su usabilidad.

La UE puso en marcha (15/02/2022) un sistema de conectividad por satélite e impulsó medidas de gestión del tráfico espacial para lograr una Europa más digital y resiliente.

La UE presenta dos iniciativas para impulsar sus ambiciones espaciales: una propuesta de Reglamento sobre una conectividad espacial segura, y una comunicación conjunta sobre un enfoque de la UE en materia de gestión del tráfico espacial.

La tecnología espacial es esencial para facilitar nuestra vida cotidiana y nos ayuda a avanzar hacia un futuro más digital, ecológico y resiliente para nuestro planeta.

El Programa Espacial de la UE, en tanto que es una de las principales potencias espaciales, ya proporciona datos y servicios valiosos con multitud de aplicaciones en nuestra vida

cotidiana, en ámbitos que van desde el transporte, la agricultura y la respuesta a las crisis hasta la lucha contra el cambio climático, entre otros muchos.

Las dos iniciativas adoptadas son resultados concretos del Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial (72), en el que se mencionan dos proyectos emblemáticos, conectividad segura y gestión de tráfico espacial, con sus tecnologías, presupuestos y normativas.

1.5.3.1.2. Telefonía móvil

La telefonía móvil es un servicio de conexión a la red telefónica pública mediante una red inalámbrica, en la cual los usuarios tienen la posibilidad de originar y recibir llamadas telefónicas.

Los teléfonos móviles funcionan enviando y recibiendo señales de radio de baja potencia. Las señales se intercambian con antenas que están conectadas a transmisores y receptores de radio, comúnmente conocidos como estaciones base de telefonía móvil.

La comunicación telefónica es posible gracias a la interconexión entre centrales móviles y públicas. Según las bandas o frecuencias en las que opera el móvil, podrá funcionar en una parte u otra del mundo. La telefonía móvil consiste en la combinación de una red de estaciones transmisoras o receptoras de radio (73) (repetidores, estaciones base o BTS) y una serie de centrales telefónicas de conmutación de 1.er y 2.º nivel (MSC y BSC respectivamente), que posibilita la comunicación entre terminales telefónicos portátiles (teléfonos móviles) o entre terminales portátiles y teléfonos (74) de la red fija tradicional.

Con la aparición de la telefonía móvil digital, fue posible acceder a páginas de Internet (75) especialmente diseñadas para móviles, conocido como tecnología WAP (76). Desde ese momento hasta la actualidad, se creó el protocolo para el envío de configuración automática del móvil para poder acceder a Internet denominado OMA Client Provisioning (77).

Actualmente es la quinta generación de telefonía móvil la que se está implementando y ha necesitado una agilización de las normativas en comunicaciones electrónicas para su implementación.

Las redes 5G son capaces de minimizar la potencia de transmisión, lo que permite optimizar los niveles de los campos electromagnéticos y garantiza el uso mínimo de energía de los dispositivos adaptados a esta tecnología para completar una comunicación satisfactoria, llegando a alcanzar hasta un 90 % en el ahorro de energía.

Para dar soporte, se ha diseñado una nueva arquitectura avanzada de radio muy eficiente a través del uso de antenas Massive MIMO, que ayuda a minimizar las transmisiones de las redes 5G y adaptarse a los requisitos del servicio. Esto es posible, entre otras cosas, gracias a que las antenas dan cobertura solo donde se necesita.

Las redes 5G están llamadas a jugar un papel fundamental en el desarrollo de las comunicaciones móviles de esta década, con sistemas mucho más potentes, veloces y con latencias mínimas. Para conseguirlo, una de las tecnologías que más éxito parece estar teniendo es la de las *small cells*. Las celdas pequeñas son nodos de acceso de radio celular de baja potencia que operan en un espectro que tiene un rango de 10 metros a unos pocos kilómetros. Son estaciones base de bajo consumo y de bajo coste, o base que se encargarán de mejorar la cobertura y hacer que la señal penetre mejor en edificios.

Es decir, para poder ofrecer todas las ventajas que prometen será necesario desplegar densas redes con estas estaciones base que, gracias a un control preciso de las interferencias entre nodos, serán capaces de ofrecer altísimas velocidades y retardos ridículos (se habla de 1 ms.)

La nueva gama de frecuencias necesarias para desplegar esta nueva generación de móviles hace preciso que en el dividendo digital generado que sobren frecuencias.

Para que la tecnología 5G funcione correctamente, los expertos decidieron que su rango óptimo de uso sería el de las bandas bajas, por eso se han tenido que mover los canales de TDT.

Pero nos podemos preguntar por qué las bandas bajas y no las bandas altas como hasta ahora, pues la respuesta es muy sencilla: al usar bandas bajas conseguimos mejor penetración de la señal en interiores, y lógicamente, tendremos mayor cobertura y mayor velocidad.

Uno de los puntos fuertes del 5G será la cobertura en casi cualquier lugar, con el objetivo de poder conectar dispositivos IoT en el interior de edificios, e incluso en parkings y otros lugares donde las bandas "altas" difícilmente llegarían.

Un detalle muy importante, es que los operadores disponen tanto de bandas de frecuencias "bajas" para llegar más lejos con una sola antena, como también bandas de frecuencias "altas" para proporcionar la máxima velocidad posible.

En entornos urbanos, seguramente tengamos disponibles varias bandas de frecuencias, y nuestro terminal móvil se conectará a la mejor banda de frecuencia y antena posible, con el objetivo de conseguir la mejor cobertura y velocidad posible. Gracias a este *roaming* podremos navegar a velocidades superiores a 500 Mbps simétricos en nuestro *smartphone* o *tablet*.

1.5.3.1.3. Frecuencias de los dispositivos wifi

Los dispositivos wifi, tienen la opción de trabajar en dos frecuencias. En teoría, el dispositivo inalámbrico debería buscar y preferir una señal de 5 GHz, pero se cambiará a una señal de 2.4 GHz si la señal de 5 GHz se deteriora por interferencia o distancia. Además, si solo una de las frecuencias se encuentra dentro del rango, el dispositivo inalámbrico se conectará a esa frecuencia. Estas frecuencias son de libre disposición.

Una conexión de 2.4 GHz viaja más lejos a velocidades más lentas, mientras que las frecuencias de 5 GHz brindan velocidades más rápidas pero menor cobertura. Su elección entre 2.4 GHz y 5 GHz dependerá de dónde y cómo use más su conexión de wifi.

1.5.4. La política de banda ancha. El ecosistema del sector digital

En el Informe especial n.° 12 2018 del Tribunal de cuentas europeo (78) argumenta y define el concepto de banda ancha, mostrando la situación del momento.

Banda ancha es el término comúnmente utilizado para referirse a velocidades de transmisión por internet más rápidas, y a otras características técnicas que permiten acceder a nuevos contenidos, aplicaciones y servicios, o también suministrarlos.

Debido a la creciente importancia de los datos digitales, las conexiones a internet adecuadas eran esenciales, no solo para que las empresas europeas siguieran siendo competitivas en la economía global, sino también, en términos más generales, para fomentar la inclusión social.

Como ya hemos introducido, el acceso a datos digitales a través de internet desempeña un papel cada vez más importante en las vidas de los ciudadanos, los gobiernos y las empresas.

El término "banda ancha" no tiene un significado técnico específico en el contexto del acceso a internet, pero se utiliza para referirse a toda infraestructura de acceso a internet de alta velocidad que está disponible en todo momento y es más rápida que el acceso tradicional mediante marcado. El tipo de infraestructura utilizado determina el límite máximo de la velocidad de conexión. Las tecnologías que dan mayor velocidad son, en principio, la fibra óptica y los móviles 5G. La velocidad real que reciban los clientes dependerá de los proveedores y de las actualizaciones técnicas.

Las iniciativas eEurope son iniciativas políticas, a escala comunitaria, dirigidas a asegurar que la Unión Europea obtenga el máximo provecho de los cambios que está produciendo la sociedad de la información, con acciones que han ido desde la liberalización de las telecomunicaciones, el establecimiento de un marco jurídico para el comercio electrónico, el apoyo a la industria y el I+D. Pero dada la velocidad a que evolucionan las tecnologías y el mercado, es necesario estar constantemente actuando con iniciativas que permitan un rápido avance de los mismos.

Con el lanzamiento de la **iniciativa eEurope 2005** se hicieron patentes las limitaciones de las infraestructuras existentes y el moderado interés de los nuevos operadores por invertir el desarrollo de otras más avanzadas.

Se podría decir que empezaba a vislumbrarse que no se podía confiar "vivir de las rentas" de las infraestructuras de telecomunicaciones acumuladas durante la época del monopolio, y que los nuevos operadores no demostraban demasiado interés en invertir, de forma masiva, en el desarrollo de otras más avanzadas, en particular en esos momentos en los que el sector se encontraba en dificultades económicas.

Era evidente que se hacía necesaria una intervención pública no solamente para impulsar el desarrollo de nuevas infraestructuras de banda ancha, sino también para fomentar su utilización de manera que la situación por la que atravesaba el sector no ralentizara el proceso de desarrollo iniciado años antes.

El propósito fue introducir acciones de profundidad para demostrar la necesidad de conexiones de alta velocidad, como, por ejemplo, la integración de las redes europeas de energía, transporte y telecomunicaciones, con actuaciones tales como que los estados miembros se esforzaran en disponer de conexiones de banda ancha para todas las administraciones públicas, ya que "la banda ancha brinda nuevas e importantes opciones desde el punto de vista de la calidad de los servicios prestados. Resultan más prácticos (y a veces, solo así son posibles) con la alta velocidad que brinda el acceso de banda ancha".

Por tanto, el desarrollo de servicios de banda ancha constituía una importante fuente de crecimiento de los ingresos, tanto para las empresas de comunicaciones de línea fija como para los operadores de cable, que sufrían un estancamiento de la demanda en sus demás servicios. El incremento de las conexiones de banda ancha generó también una demanda significativa de equipos, lo que favoreció, a su vez, a los fabricantes.

La combinación de intereses económicos y sociales en el desarrollo de las conexiones de alta velocidad impulsó a numerosos gobiernos a tomar medidas específicas para estimular su desarrollo. Numerosos estados miembros, en efecto, elaboraron "estrategias de banda ancha" específicas.

El período posterior a 2008 presentó una situación económica y social muy deteriorada por la crisis económica de ese año, donde quebraban o se fusionaban entidades financieras en todo el planeta, desde EE. UU., hasta prácticamente en todos los estados miembros, y donde los estados insuflaban subvenciones millonarias a dichas entidades. La crisis mencionada había destruido años de progreso económico y social, y dejado al descubierto los puntos débiles estructurales de la economía de Europa.

Para facilitar soluciones, la Comisión Europea propuso una agenda digital cuyo principal objetivo consistió en desarrollar un mercado único digital para dirigir a Europa hacia un crecimiento inteligente, sostenible e integrador.

Los obstáculos que iban a dificultar la agenda digital fueron, sobre todo, la fragmentación de los mercados digitales, la falta de interoperabilidad, el incremento de la ciberdelincuencia y el riesgo de escasa confianza en las redes, la ausencia de inversión en las redes, la insuficiencia de los esfuerzos de investigación e innovación, las carencias en la alfabetización y la capacitación digitales, la pérdida de oportunidades para afrontar los retos sociales, etc.

Dos son las agendas digitales (2010-2020 y 2020-2030) implementadas por la UE, basándose en que la economía digital crece siete veces más deprisa que el resto de la economía, y necesitando para ello de decenas de millones más, de puestos de trabajo que requieran competencias en tecnologías TIC.

La primera de estas agendas digitales se centró en mejorar el acceso de los consumidores y las empresas a los bienes y servicios digitales en Europa, dotando a tal efecto a la Unión de un avanzado sistema de derechos de los usuarios y protección de los consumidores y empresas; en concreto:

- Unas **tarifas más bajas para las comunicaciones electrónicas** (Reglamento (UE) n.° 531/2012 (79)), y la **supresión de los costes de itinerancia** el 14 de junio de 2017 (régimen de "Itinerancia como en casa").
- Una **mejor conectividad a Internet** para todos con una cobertura de banda ancha básica completa, debida fundamentalmente a los avances en la banda ancha móvil y por satélite, con el fin de desarrollar una conectividad de alta velocidad para los principales motores socioeconómicos.
- Una **mayor protección de los consumidores en los servicios de telecomunicaciones** mediante la adopción de **legislación sobre protección de la privacidad** (Directiva 2009/136/CE) y de los datos (Directiva 95/46/CE), **reforzada con el nuevo marco regulador sobre protección de datos** (Reglamento (UE) 2016/679 (63) y Directiva (UE) 2016/680 (80)).

Con el fin de crear las condiciones adecuadas para que prosperasen las redes y los servicios digitales, el Parlamento Europeo reforzó el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), como ya se ha dicho, que facilita la cooperación entre los reguladores nacionales y la comisión, promueve buenas prácticas y enfoques comunes, y armoniza la regulación de las comunicaciones en el mercado único (Reglamento (UE) 2018/1971 (51)).

Esta estrategia tenía por objeto maximizar el potencial de crecimiento de la economía digital, fomentando las competencias digitales y la informática de alto rendimiento, digitalizando la industria y los servicios, desarrollando la inteligencia artificial (IA) y modernizando los servicios públicos.

Se adoptaron nuevas normas sobre el **bloqueo geográfico** (Reglamento (UE) 2018/302 (81)) y la **portabilidad de los servicios digitales** (Reglamento (UE) 2017/1128 (82)) para permitir que los consumidores también accedieran a los servicios de contenidos en línea adquiridos en un estado miembro de la UE cuando visitan otro.

Además de los nuevos marcos reguladores sobre protección de datos (Reglamento (UE) 2016/679 (63) y Directiva (UE) 2016/680 (80)) mencionados, la UE ha adoptado varias medidas para facilitar el desarrollo de una economía "ágil" en materia de datos, a saber:

- *El Reglamento sobre la* ***libre circulación de datos no personales*** (los datos no personales son definidos como aquellos datos que no están relacionados con una persona física, identificada o identificable, número de registro mercantil, dirección de correo electrónico, del tipo info@empresa.com, datos anonimizados.) (Reglamento (UE) 2018/1807 (83)), que permite a las empresas y a las administraciones públicas almacenar y tratar datos no personales en las ubicaciones que elijan.
- *La* ***Ley de Ciberseguridad*** (Reglamento (UE) 2019/881 (84)), que refuerza la Agencia de la UE para la Ciberseguridad (**ENISA**) y establece un marco de **certificación en ciberseguridad** para productos y servicios.
- L*a Directiva relativa a los* ***datos abiertos*** (datos digitales de carácter público que son accesibles en línea, y pueden ser usados, reutilizados y redistribuidos por cualquier interesado) (Directiva (UE) 2019/1024 (85)), que establece normas comunes aplicables

a un mercado europeo de datos en manos de administraciones públicas.

Por otra parte, la segunda agenda digital se centró en los profundos cambios introducidos por las tecnologías digitales, el papel esencial de los servicios y mercados digitales y las nuevas ambiciones tecnológicas y geopolíticas de la UE.

Sobre la base de dos comunicaciones estratégicas, a saber, "Configurar el futuro digital de Europa" (86) y "La década digital de Europa" (87), la Comisión estableció las acciones específicas que emprenderá para contribuir a la creación de servicios y mercados digitales seguros y protegidos.

El 9 de marzo de 2021, la UE propuso una "**Brújula Digital**" (COM(2021)0118) (88) con cuatro objetivos digitales que deben alcanzarse de aquí a 2030:

- **Competencias**: al menos el 80 % de los adultos deberían poseer competencias digitales básicas, y debería haber 20 millones de especialistas en TIC empleados en la UE; además, debería aumentar el número de mujeres que asuman este tipo de puestos de trabajo.
- **Actividad empresarial**: el 75 % de las empresas deberían utilizar servicios de computación en la nube, macrodatos e IA; más del 90 % de las pequeñas y medianas empresas (pymes) de la Unión deberían alcanzar al menos un nivel básico de intensidad digital; y debería duplicarse el número de unicornios de la UE (las **empresas unicornio** son aquellas compañías que logran generar un valor de 1.000 millones de dólares durante su primer año de lanzamiento al mercado, aún sin haber entrado en la bolsa de valores, y sin contar con la financiación de inversores u otras empresas más grandes).
- **Infraestructura**: todos los hogares de la UE deberían contar con una conectividad de altísima velocidad y todas las zonas pobladas deberían disponer de cobertura 5G; la producción de semiconductores de vanguardia y sostenibles en Europa debería suponer al menos el 20 % de la producción mundial; en la UE deberían desplegarse 10.000 nodos de proximidad con alto grado de seguridad y neutros desde el punto de vista climático, y Europa debería contar con su primer ordenador cuántico.
- **Servicios públicos**: todos los servicios públicos esenciales deberían estar disponibles en línea; todos los ciudadanos tendrán acceso a sus historiales médicos electrónicos, y el 80 % de los ciudadanos deberán utilizar una solución de identidad electrónica.

La Unión Europea plantea programas de apoyo para potenciar innovación en estos temas siendo el más destacado El programa Europa Digital (89), un nuevo programa de financiación de la UE en materia de tecnología digital, con un presupuesto global previsto de 7.500 millones € para el período 2021-2027, que debe proporcionar financiación estratégica para apoyar proyectos en cinco ámbitos:

- Supercomputación.
- Inteligencia artificial.
- Ciberseguridad.
- Competencias digitales avanzadas.
- La garantía de un amplio uso de las tecnologías digitales en todos los ámbitos de la economía y la sociedad, también a través de los centros de innovación digital.

El fondo se complementará con otros programas de la UE, como Horizonte Europa (90), el Mecanismo "Conectar Europa" para la infraestructura digital, el Mecanismo de Recuperación y Resiliencia (91) y el mecanismo de los Fondos Estructurales.

En el contexto de la recuperación económica tras la pandemia de la COVID-19, los estados miembros deben asignar al menos el 20 % de sus fondos de recuperación a proyectos que digitalicen sus economías y sociedades (Reglamento UE 2021/694) (92).

Se considera que el ámbito de la IA desempeña un papel fundamental, y se prevé que aportará múltiples beneficios sociales y

económicos a una amplia gama de sectores. Por ello, en octubre de 2020, el Parlamento Europeo adoptó tres instrumentos legislativos sobre la IA que abarcan la ética (93), la responsabilidad civil (94) y la propiedad intelectual (95), y solicitó a la Comisión que estableciera un marco jurídico europeo global y preparado para el futuro, constituido por principios éticos respecto al desarrollo, el despliegue y el uso de la IA, la robótica y las tecnologías conexas, dando lugar a la nueva ley de Inteligencia Artificial (COM(2021)0206) (96).

La puesta en común de datos es el segundo eje principal en el que se basa la nueva agenda digital para Europa. Al tiempo que persigue la innovación basada en los datos, la UE se propone salvaguardar el equilibrio entre la libre circulación de los datos y la preservación de la privacidad, la seguridad, la protección y las normas éticas. Esto incluye el examen de diversas formas de utilizar y compartir datos no personales con el fin de desarrollar nuevas tecnologías y modelos de negocio rentables.

En este sentido, en febrero de 2020, se publicó una Estrategia Europea de Datos (97), junto con el Libro Blanco sobre la IA.

Otro pilar de la Estrategia Europea de Datos es el Reglamento de Gobernanza de Datos europeo (Reglamento (UE) 2022/868) (98) que se publicó en el Diario Oficial de la UE el 3 de junio de 2022, entró en vigor el 23 de junio de 2022 y es aplicable a partir de septiembre de 2023. Tiene por objeto aumentar la disponibilidad y la reutilización de los datos y la confianza en el intercambio de estos.

Otro aspecto de la estrategia digital es la creación de un mercado único digital más seguro y abierto, que proteja los derechos fundamentales de los usuarios y establezca condiciones de competencia equitativas para las empresas.

Por tal motivo, el 15 de diciembre de 2020, la Comisión presentó al Parlamento y al Consejo su propuesta de paquete de Ley de Servicios Digitales (99) de conformidad con el procedimiento de codecisión.

El paquete consta de dos iniciativas legislativas: la Ley de Servicios Digitales (81) (101) y la Ley de Mercados Digitales (102) (103), cuyo objetivo es mejorar las normas que rigen los servicios digitales en la Unión.

Una vez en vigor, completarán el mercado único digital mediante un conjunto coherente de nuevas normas aplicables en toda la UE.

De hecho, la Ley de Servicios Digitales establece normas inequívocas en materia de responsabilidad y de rendición de cuentas para los prestadores de servicios intermediarios (todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos) y, en particular, para las plataformas en línea como los mercados y las redes sociales.

Las plataformas en línea de muy gran tamaño estarán sujetas a obligaciones específicas debido a los riesgos particulares que plantean en la difusión de contenidos ilegales y nocivos.

La Ley de Servicios Digitales establece las normas sobre lo que se permitirá hacer en la UE a las empresas designadas como “guardianes de acceso” (plataformas que tienen la facultad de actuar como creadores de normas privadas y pueden imponer unilateralmente condiciones a sus empresas usuarias).

El Reglamento se aplicará a las grandes empresas que prestan los denominados servicios de plataformas básicas más propensos a prácticas desleales. Estos incluyen servicios de intermediación en línea, redes sociales, motores de búsqueda, sistemas operativos, servicios de publicidad en línea, computación en la nube y servicios de intercambio de vídeos, que cumplen los criterios pertinentes para ser designados como “guardianes de acceso”.

Generar confianza en el entorno en línea es clave para el desarrollo social y económico y, por tanto, constituye una prioridad adicional.

1.6. EL LIBRO BLANCO: ¿CÓMO GESTIONAR LAS NECESIDADES DE INFRAESTRUCTURA DIGITAL DE EUROPA? "LA LEY DE REDES DIGITALES, EL NUEVO RETO"

La Comisión Europea, finalizando la legislatura de 2019-2024 es consciente de la urgencia en solucionar las limitaciones que está sufriendo la UE en la economía global con la brecha tecnológica con EE. UU. y China, y con el deterioro de las relaciones geopolíticas en cuanto a seguridad. Trabaja con una serie de posibles medidas de fomento de la innovación, la seguridad y la resiliencia de las infraestructuras digitales. La competitividad futura de la economía europea depende de estas infraestructuras y servicios de redes digitales avanzados, ya que una conectividad rápida, segura y generalizada es esencial para la implantación de las tecnologías que nos acercarán al futuro.

Primeramente, la Comisión Europea lanzó una consulta, el 23 de marzo de 2023, sobre el futuro del sector de la conectividad y sus infraestructuras a todas las partes interesadas, cuyas conclusiones se publicaron en octubre del mismo año.

Junto a la consulta, la Comisión también presentó la Ley de las Infraestructuras de Gigabit, consiguiendo un acuerdo político un año después, 5 de febrero de 2024. Lo que pretende este Reglamento es simplificar y acelerar el despliegue de redes de muy alta capacidad, reduciendo la burocracia y el coste del mismo (104).

A la vez, se adoptó la recomendación sobre la promoción por vía normativa de la conectividad de *gigabit*, para facilitar a las autoridades de los estados miembros de reglamentación y orientación cómo formular las obligaciones de solución de acceso mayorista para los operadores con peso significativo en el mercado (105).

También ha adoptado medidas para reforzar la conectividad troncal a través de entidades privadas, como asociaciones, que garantizan una conectividad de alta calidad en toda la Unión, incluidas las regiones ultraperiféricas, las islas, los estados miembros con costas, y los países y territorios de ultramar. Del mismo modo, sostienen infraestructuras fundamentales como los cables submarinos, financiadas con cargo al Mecanismo "Conectar Europa" (106).

A todo ello, la Comisión sigue presentando una serie de posibles medidas de fomento de innovación, la seguridad y la resiliencia de las infraestructuras digitales de acuerdo con los informes Letta (107) y Draghi (108) sobre mercado único competitivo, donde se suma a las cuatro libertades fundamentales que le caracterizan (libertad de movimiento de personas, bienes, servicios y capital) la libertad de investigar, explorar y crear sin límites. "Este quinto pilar capturará los elementos intangibles de la economía digital y los beneficios de la economía circular necesaria para combatir el cambio climático que el mercado único actual no tiene en cuenta".

Durante el primer trimestre de 2024 lanza un paquete de conectividad digital para abrir un debate con las partes interesadas, los estados miembros y socios afines, con propuestas para configurar la futura acción política de la UE y lograr un consenso en este tema:

- El Libro Blanco "¿Cómo abordar con éxito las necesidades de infraestructura digital de Europa?" analiza los retos a los que se enfrenta Europa en lo relativo al despliegue de las futuras redes de conectividad, y presenta posibles hipótesis para atraer inversiones, fomentar la innovación, mejorar la seguridad y lograr un verdadero mercado único digital (109).
- La recomendación sobre la seguridad y la resiliencia de las infraestructuras de cables submarinos presenta un conjunto de medidas a nivel nacional y de la UE destinadas a mejorar la seguridad y la fortaleza de los cables submarinos mediante una mejor coordinación en toda la UE, tanto en

términos de gobernanza como de financiación (110).

El Libro Blanco plantea una serie de propuestas, como que la UE debe fomentar una comunidad dinámica de innovadores europeos mediante el estímulo del fomento de infraestructuras de conectividad integrada e informática colaborativa. Para alcanzar este objetivo, se prevé la creación de una red de "computación colaborativa conectada" (red3C) con el fin de crear infraestructuras y plataformas integradas de extremo a extremo para las telecomunicaciones en la nube y en el borde, que podrían servir para el fomento de tecnologías innovadoras y aplicaciones de inteligencia artificial con diversos usos. También es esencial aprovechar mejor las sinergias entre las iniciativas existentes, tales como el PIICE, de infraestructura y servicios en la nube de nueva generación, y los programas de financiación del Mecanismo "Conectar Europa" y Europa Digital. En definitiva, es primordial apoyar la creación de un ecosistema colaborativo de conectividad y computación.

Además, la UE debe aprovechar todo el potencial del mercado único digital de las telecomunicaciones, teniendo en cuenta que el sector de las telecomunicaciones es el único segmento del ecosistema digital que no está dominado por empresas norteamericanas, mediante el estudio de medidas que garanticen una verdadera igualdad de condiciones de competencia y un nuevo examen del ámbito de aplicación y los objetivos de su actual normativa. Esta reflexión debe tener en cuenta la convergencia tecnológica entre las telecomunicaciones y la nube (las cuales están sujetas, no obstante, a normativas diferentes), y la necesidad de velar por que todos los agentes económicos que inviertan en infraestructuras digitales puedan alcanzar el tamaño necesario para realizar inversiones masivas. Para ello, podría ser necesario un enfoque más armonizado de los procedimientos de autorización de los operadores de telecomunicaciones, una gobernanza más integrada a escala de la Unión para el espectro, y posibles cambios en la política de acceso mayorista. En resumen, hay que crear estructuras de mercado favorables a la inversión.

Además, para proteger la infraestructura informática y de red de Europa, que constituye un elemento esencial de nuestra seguridad económica, la UE debe incentivar el despliegue y mejorar la seguridad y la fortaleza de las infraestructuras estratégicas de cable submarino.

El resultado recogido en el Libro Blanco expresa a la vez un gran reto y una gran preocupación en términos de seguridad económica y autonomía estratégica. El Libro Blanco es un paso crucial en el camino hacia un futuro digital europeo más seguro y próspero.

Enrico Letta resalta en su informe la urgente necesidad de unir mercados, simplificar la regulación y permitir alcanzar la escala adecuada a las empresas europeas. En este contexto, es esencial establecer un marco regulatorio sólido que fomente la innovación y la competitividad en el sector de las comunicaciones digitales. En la búsqueda de este objetivo, una Ley de Redes Digitales bien enfocada adquiere una mayor relevancia para convertir al sector de las telecomunicaciones europeo en una palanca para avanzar en la consecución del mercado único europeo.

En definitiva, el sector de las telecomunicaciones afronta desafíos significativos en términos de estructuras de mercado y paradigmas regulatorios. El nuevo instrumento regulatorio propuesto por la Comisión Europea, la Ley de Redes Digitales (DNA), si aborda en profundidad los desequilibrios actuales, será imprescindible para afrontar los problemas de escala del sector, la necesidad de un nuevo paradigma regulatorio y de un campo de juego equilibrado que permita el surgimiento de nuevos modelos de negocio. Este instrumento no solo es necesario, sino urgente.

La nueva Comisión Europea se plantea esta Ley de Redes Digitales para finales de 2025; veremos si es valiente en su diseño y permita dar un salto cualitativo en este segmento del ecosistema digital europeo, por lo que va a ser un quinquenio muy importante en el desarrollo de la sociedad digital europea, así como en la política de telecomunicaciones.

1.7. REFERENCIAS BIBLIOGRÁFICAS

1. Consejo de Ministros. Informe del Grupo de Trabajo "Política de investigación científica y técnica", grupo especializado Telecomunicaciones. Bruselas; 1969 abr 9.
2. Unión Internacional de las Telecomunicaciones (UIT), Comité consultivo internacional de las radiocomunicaciones (CCIR), Comité consultivo internacional de telegrafía y telefonía (CCITT), Conferencia europea de correos y telecomunicaciones (CEPT).
3. European Cooperation in Science & Technology (COST). Red intergubernamental europea de coordinación de la investigación; 1971.
4. Spinelli M. La coordinación de los proyectos de desarrollo de las redes de telecomunicación en la Comunidad [declaración]. Luxemburgo: Parlamento Europeo; 1972 may 9.
5. Decisión del Consejo de 18 de marzo de 1975.
6. Comisión Europea. La Sociedad Europea encara el reto de las nuevas tecnologías de la información: una respuesta comunitaria [comunicación]. Bruselas; 1979 nov 26.
7. Comisión Europea. Recomendaciones concernientes a las Telecomunicaciones [informe]. Bruselas; 1980 sep 1.
8. Parlamento Europeo. Moción para una resolución sobre política común en el campo de las telecomunicaciones. Bruselas; 1982 may 11.
9. Consejo Europeo. Directiva 83/189/CEE por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas. Diario Oficial de las Comunidades Europeas; 1983 mar 28.
10. Comisión Europea. Telecomunicaciones [comunicación COM(83) 329 final]. Bruselas; 1983 jun 9.
11. Parlamento Europeo. Informe elaborado en nombre de la Comisión de Asuntos Económicos y Monetarios sobre telecomunicaciones [documento 1-1477/83]. Bruselas; 1984 mar 3.
12. Comisión Europea. Comunicación sobre Telecomunicaciones [COM(84)277]. Bruselas; 1984 may 18.
13. Consejo Europeo. Recomendación 84/549/CEE relativa a la puesta en marcha de la armonización en el Campo de las Telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1984 nov 12.
14. Consejo Europeo. 979 sesión del Consejo -Industria/Siderurgia [nota de prensa]. Bruselas; 1984 dic 17.
15. Comisión Europea. Comunicación sobre el Estado de la Política Comunitaria de Telecomunicaciones [COM(85) Final]. Bruselas; 1985 may 30.
16. Consejo Europeo. Resolución 85/L136/01 relativa a una nueva aproximación en materia de armonización y de normalización. Diario Oficial de las Comunidades Europeas; 1985 may 7.

17. Comunidad Económica Europea. Programa relativo al desarrollo de determinadas regiones desfavorecidas mediante un mejor acceso a los servicios avanzados de telecomunicaciones (STAR); 1987-1991.

18. Consejo Europeo. Reglamento (CEE) Nº 33000/86 por el que se establece un programa Comunitario relativo al desarrollo de determinadas regiones desfavorecidas de la Comunidad mediante un mejor acceso a los servicios avanzados de telecomunicaciones (Programa STAR). Diario Oficial de las Comunidades Europeas; 1986 nov 27.

19. Comisión Europea. Comunicación sobre la Política Comunitaria de las Telecomunicaciones [COM(86) 325 final]. Bruselas; 1986 jun 5.

20. Consejo Europeo. Decisión 87/95/CEE relativa a la normalización en el campo de las tecnologías de la información y las telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1986 dic 27.

21. Comisión Europea. Hacia una economía europea dinámica. Libro verde sobre el desarrollo del mercado común para servicios y equipos de telecomunicaciones [COM(87) 290 final]. Bruselas; 1987.

22. Comisión Europea. Directiva 88/301/CEE relativa a la competencia en los mercados de terminales de telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1988 may 16.

23. Consejo Europeo. Directiva 91/263/CEE relativa a la aproximación de las legislaciones de los Estados Miembros sobre equipos terminales, incluidos el reconocimiento mutuo. Diario Oficial de las Comunidades Europeas; 1991 abr 29.

24. Consejo Europeo. Directiva 92/44/CEE relativa a la armonización de las condiciones de acceso y utilización de las líneas arrendadas suministradas a través de las redes públicas de telecomunicación. Diario Oficial de las Comunidades Europeas; 1992.

25. Parlamento Europeo, Consejo Europeo. Directiva 97/33/CE relativa a la interconexión en las telecomunicaciones en lo que respecta a garantizar el servicio universal y la interoperabilidad mediante la aplicación de los principios de la oferta de red abierta (ONP). Diario Oficial de las Comunidades Europeas; 1997 jun 30.

26. Comisión Europea. Hacia una economía europea dinámica, Libro verde sobre el desarrollo del mercado común de servicios y equipos de telecomunicaciones [COM/87/290]. Bruselas; 1987.

27. Consejo Europeo. Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo. Bruselas; 1994 may 26.

28. Comisión Europea. Europa en marcha hacia la sociedad de la información [COM(94)347 final]. Bruselas; 1994 jul 19.

29. Parlamento Europeo. Europa y la sociedad global de la información - Recomendaciones al Consejo Europeo [A4-0073/94]. Bruselas; 1994 nov 15.

30. Parlamento Europeo, Consejo Europeo. Directiva 94/10/CE por la que se modifica por segunda vez la Directiva 83/189/CEE sobre procedimiento de información en materia de normas y reglamentaciones técnicas. Diario Oficial de las Comunidades Europeas; 1994 mar 23.

31. Comisión Europea. Libro verde sobre la liberalización de las infraestructuras de telecomunicaciones y redes de televisión por cable. Primera parte [COM(94) 440 final]. Bruselas; 1994 oct 25.

32. Comisión Europea. Libro verde sobre la liberalización de las infraestructuras de telecomunicaciones y redes de televisión por cable. Segunda parte [COM(94) 682 final]. Bruselas; 1995 ene 25.

33. Consejo Europeo. Resolución 94/C 379/03 relativa a los principios y al calendario de la liberalización de las infraestructuras de telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1994 dic 22.

34. Comisión Europea. El servicio universal de telecomunicaciones ante la perspectiva de un entorno plenamente liberalizado [COM(96) 73 final]. Bruselas; 1996 mar 13.

35. Parlamento Europeo, Consejo Europeo. Directiva 97/13/CE relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1997 abr 10.

36. Comisión Europea. Libro verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información [COM(97) Versión 3]. Bruselas; 1997 dic 3.

37. Comisión Europea. Libro verde sobre la política en materia de espectro radioeléctrico [COM(1998) 596 final]. Bruselas; 1998 dic 9.

38. Pérez Martínez J. Internet. La globalización de las comunicaciones electrónicas Desafíos de la gobernanza de internet; Telos 100, 17-21; 2015 feb-may.

39. Parlamento Europeo, Consejo Europeo. Reglamento (CE) nº 2887/2000 sobre el acceso desagregado al bucle local. Diario Oficial de las Comunidades Europeas; 2000 dic 18.

40. Alabau A, Guijarro L. La política de las comunicaciones electrónicas de la Unión Europea. Valencia: Editorial UPV; 2011.

41. Walden I. Telecomunications Law and Regulation. 5th ed. Oxford: Oxford University Press; 2018.

42. Comisión Europea. i2010 - Una sociedad de la información europea para el crecimiento y el empleo [COM(2005) 229 final]. Bruselas; 2005 jun 1.

43. Comisión Europea. Directiva 90/388/CEE relativa a la competencia en los mercados de servicios de telecomunicaciones. Diario Oficial de las Comunidades Europeas; 1990 jun 28.

44. Comisión Europea. Directiva 1999/64/CE por la que se modifica la Directiva 90/388/CEE con objeto de garantizar que las redes de telecomunicaciones y de televisión por cable propiedad de un único operador sean entidades jurídicas independientes. Diario Oficial de las Comunidades Europeas; 1999 jun 23.

45. Consejo Europeo. Directiva 89/552 modificada por directiva 97/36/CE sobre liberalización de las telecomunicaciones y desarrollo de la Sociedad de la Información. Diario Oficial de las Comunidades Europeas.

46. Unión Europea. Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 mar 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de Servicios de Comunicación Audiovisual); Art. 1. Diario Oficial de la Unión Europea. 2010 abr 15;L95:1-24.

47. Parlamento Europeo, Consejo Europeo. Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual. Diario Oficial de la Unión Europea; 2010 mar 10.

48. Parlamento Europeo, Consejo Europeo. Directiva (UE) 2018/1808 por la que se modifica la Directiva 2010/13/UE sobre servicios de comunicación audiovisual [Internet]. Diario Oficial de la Unión Europea; 2018 nov 14. Disponible en: https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:32018L1808

49. Comisión Europea. Una estrategia para el mercado único digital de Europa [COM/2015/0192]. Bruselas; 2015.

50. Parlamento Europeo, Consejo Europeo. Directiva (UE) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas. Diario Oficial de la Unión Europea; 2018 dic 11.

51. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2018/1971 por el que se establecen el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Agencia de apoyo al ORECE [Internet]. Diario Oficial de la Unión Europea; 2018 dic 11. Disponible en: http://ec.europa.eu/digital-single-market/en/telecoms y http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:4379982

52. Parlamento Europeo, Consejo Europeo. Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso) [Internet]. Diario Oficial n° L 108 de 24/04/2002 p. 0007-0020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:32002L0019

53. Parlamento Europeo, Consejo Europeo. Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) [Internet]. Diario Oficial n° L 108 de 24/04/2002 p. 0021-0032. Disponible en: https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:32002L0020

54. Parlamento Europeo, Consejo Europeo. Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [Internet]. Diario Oficial n° L 108 de 24/04/2002 p. 0033-0050. Disponible en: https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:32002L0021

55. Parlamento Europeo, Consejo Europeo. Decisión n° 243/2012/UE del Parlamento Europeo y del Consejo, por la que se establece un programa plurianual de política del espectro radioeléctrico [Internet]. Estrasburgo: 2012 mar 14. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:310502_1

56. Parlamento Europeo, Consejo Europeo. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [Internet]. Diario Oficial n° L 201 de 31/07/2002 p. 0037-0047. Disponible en: https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=celex:32002L0058

57. Protección de datos en el sector de las comunicaciones electrónicas | EUR-Lex [Internet]. Europa.eu. 2020. Disponible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=LEGISSUM:l24120

58. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2021/1232 sobre tratamiento de datos personales con fines de lucha contra los abusos sexuales de menores en línea. Diario Oficial de la Unión Europea; 2021 jul 14.

59. Parlamento Europeo, Consejo Europeo. Reglamento (CE) n° 1211/2009 por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Oficina. Diario Oficial de la Unión Europea; 2009 nov 25.

60. Comisión Europea. Una Estrategia para el Mercado Único Digital de Europa [COM(2015) 192 final]. Bruselas; 2015 may 6.

61. Comisión Europea. Decisión 2002/622/CE por la que se crea un Grupo de política del espectro radioeléctrico. Diario Oficial de las Comunidades Europeas; 2002 jul 26.

62. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2018/1725 relativo a la protección de datos personales por las instituciones de la Unión. Diario Oficial de la Unión Europea; 2018 oct 23.

63. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (Reglamento general de protección de datos). Diario Oficial de la Unión Europea; 2016 abr 27.

64. Parlamento Europeo, Consejo Europeo. Directiva 2010/13/UE sobre la coordinación de disposiciones relativas a la prestación de servicios de comunicación audiovisual. Diario Oficial de la Unión Europea; 2010 mar 10.

65. Parlamento Europeo, Consejo Europeo. Reglamento (UE) nº 526/2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA). Diario Oficial de la Unión Europea; 2013 may 21.

66. Parlamento Europeo, Consejo Europeo. Reglamento (UE) nº 912/2010 por el que se crea la Agencia del GNSS Europeo. Diario Oficial de la Unión Europea; 2010 sep 22.

67. Parlamento Europeo, Consejo Europeo. Reglamento (CE) N° 2006/2004 sobre la cooperación entre las autoridades nacionales de protección de los consumidores. Diario Oficial de la Unión Europea; 2004 oct 27.

68. Parlamento Europeo, Consejo Europeo. Decisión nº 676/2002/CE sobre marco regulador de la política del espectro radioeléctrico (Decisión espectro radioeléctrico). Diario Oficial de las Comunidades Europeas; 2002 mar 7.

69. Parlamento Europeo, Consejo Europeo. Decisión nº 243/2012/UE por la que se establece un programa plurianual de política del espectro radioeléctrico. Diario Oficial de la Unión Europea; 2012 mar 14.

70. Comisión Europea. Decisión 2019/C 196/08 por la que se constituye el Grupo de política del espectro radioeléctrico. Diario Oficial de la Unión Europea; 2019 jun 11.

71. European Commission - EUR-Lex [Internet]. Europa.eu. 2025. Disponible en: http://eur-lex.europa.eu/summary/glossary/european_commission.html

72. Comisión Europea. Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial [COM(2021) 70 final]. Bruselas; 2021 feb 22.

73. Radiofrecuencia [Internet]. Wikipedia. 2020. Disponible en: https://es.wikipedia.org/wiki/Radiofrecuencia

74. Colaboradores de los proyectos Wikimedia. Dispositivo de telecomunicación - Teléfono [Internet]. Wikipedia.org. Wikimedia Foundation, Inc.; 2003. Disponible en: https://es.wikipedia.org/wiki/Tel%C3%A9fono

75. Colaboradores de los proyectos Wikimedia. Conjunto descentralizado de redes de comunicación interconectadas de alcance mundial - Internet [Internet]. Wikipedia.org. Wikimedia Foundation, Inc.; 2002. Disponible en: https://es.wikipedia.org/wiki/Internet

76. Wireless Application Protocol (WAP) [Internet]. Wikipedia.org. Wikimedia Foundation, Inc.; 2003. Disponible en: https://es.wikipedia.org/wiki/Wireless_Application_Protocol

77. OMA Client Provisioning [Internet]. Wikipedia.org. Wikimedia Foundation, Inc.; 2013. Disponible en: https://es.wikipedia.org/wiki/OMA_Client_Provisioning

78. Tribunal de Cuentas Europeo. La banda ancha en los Estados miembros de la UE: pese a los avances, no se cumplirán todos los objetivos de la Estrategia Europa 2020 [Informe especial nº 12]. Luxemburgo: 2018.

79. Parlamento Europeo, Consejo Europeo. Reglamento 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión (versión refundida) Texto pertinente a efectos del EEE - EUR-Lex [Internet]. Europa.eu. 2012. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32012R0531

80. Parlamento Europeo, Consejo Europeo. Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo - EUR-Lex [Internet]. Europa.eu. 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02016L0680-20160504

81. Parlamento Europeo, Consejo Europeo. Reglamento 2018/302 sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.° 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (UE) - EUR-Lex [Internet]. Europa.eu. 2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32018R0302

82. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo de 14 de junio de 2017 relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior - EUR-Lex [Internet]. Europa.eu. 2017. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02017R1128-20170630

83. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea - EUR-Lex [Internet]. Europa.eu. 2018. Disponible en: https://eur-lex.europa.eu/eli/reg/2018/1807/oj

84. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad») - EUR-Lex [Internet]. Europa.eu. 2019. Disponible en: https://eur-lex.europa.eu/eli/reg/2019/881/oj

85. Parlamento Europeo, Consejo Europeo. Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público - EUR-Lex [Internet]. Europa.eu. 2019. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1561563110433&uri=CELEX:32019L1024

86. Comisión Europea. Configurar el futuro digital de Europa [Internet]. Comisión Europea; 2019. Disponible en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_es

87. Comisión Europea. La década digital de Europa: Metas para 2030 | Comisión Europea [Internet]. Comisión Europea. 2019. Disponible en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

88. Comisión Europea. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de la regiones Brújula Digital 2030: el enfoque de Europa para el Decenio Digital. COM(2021)0118 [Internet]. European Commission. 2021. Disponible en: https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf

89. European Commission. Digital Programme | Shaping Europe's digital future [Internet]. digital-strategy.ec.europa.eu. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

90. European Commission. Horizon Europe [Internet]. Research and innovation. 2025. Disponible en: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_es

91. European Commission. Connecting Europe Facility - CEF Digital [Internet]. Shaping Europe's digital future. 2021. Disponible en: https://digital-strategy.ec.europa.eu/en/activities/cef-digital

92. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2021/694 del Parlamento europeo y del Consejo de 29 de abril de 2021 por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240 - EUR-Lex [Internet]. Europa.eu. 2021. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021R0694&from=ES

93. Textos aprobados - Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas - Martes 20 de octubre de 2020 [Internet]. Europa.eu. 2020. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html

94. Parlamento Europeo. Textos aprobados - Régimen de responsabilidad civil en materia de inteligencia artificial. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial (2020/2014(INL)) [Internet]. Europa.eu. 2020. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.pdf

95. Textos aprobados - Derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial - Martes 20 de octubre de 2020 [Internet]. Europa.eu. 2020. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_ES.html

96. Parlamento Europeo, Consejo Europeo. Reglamento del Parlamento europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión - COM(2021)0206 - EN - EUR-Lex [Internet]. Europa.eu. 2021. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1623335154975&uri=CELEX:52021PC0206

97. European Commission. Strategy for Data | Shaping Europe's digital future [Internet]. digital-strategy.ec.europa.eu. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

98. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) - EN - EUR-Lex [Internet]. Europa.eu. 2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32022R0868

99. Parlamento Europeo, Consejo Europeo. Propuesta de Reglamento del Parlamento europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE | COM/2020/825 final - EN - EUR-Lex [Internet]. Europa.eu. 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2020:825:FIN

100. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales). Diario Oficial de la Unión Europea; 2022 oct 19.

101. Parlamento Europeo. Ley de Servicios Digitales | 2020/0361(COD). Amending Directive 2000/31 1998/0325(COD) [Internet]. Europa.eu. 2020. Disponible en: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0361(COD)

102. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2022/1925 sobre mercados disputables y equitativos en el sector digital (Reglamento de Mercados Digitales). Diario Oficial de la Unión Europea; 2022.

103. Parlamento Europeo. Ley de mercados digitales | 2020/0374(COD) [Internet]. Europa.eu. 2020. Disponible en: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0374(COD)

104. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2024/1309 por el que se establecen medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de gigabit. Diario Oficial de la Unión Europea; 2024 abr 29.

105. Comisión Europea. Recomendación sobre la promoción regulatoria de la conectividad de gigabit [C(2024) 523 final]. Bruselas; 2024 feb 6.

106. Parlamento Europeo, Consejo Europeo. Reglamento (UE) 2021/1153 por el que se establece el Mecanismo «Conectar Europa». Diario Oficial de la Unión Europea; 2021 jul 7.

107. Letta E. El futuro del mercado único europeo: Mucho más que un mercado [informe]. Bruselas: Consejo Europeo; 2024 may 22.

108. Draghi M. Una estrategia competitiva para Europa [informe]. Bruselas: Comisión Europea; 2024.

109. Comisión Europea. ¿Cómo abordar con éxito las necesidades de infraestructura digital de Europa? [Libro Blanco, COM(2024) 81 final]. Bruselas; 2024 feb 21.

110. Comisión Europea. Recomendación sobre la seguridad y la resiliencia de las infraestructuras de cables submarinos [C(2024) 1181 final]. Bruselas; 2024 feb 26.

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

2

El futuro de las telecomunicaciones europeas

Juan Luis Redondo Maíllo

2.1. UN SECTOR EN PROFUNDA TRANSFORMACIÓN

Para muchas generaciones de ingenieros la imagen de una red de telecomunicaciones ha sido la de la red que nos permitía mantener conversaciones utilizando un teléfono fijo. Esta red nos ha acompañado a lo largo de más de 100 años, y aún hoy pervive en la imaginación de todos nosotros. Los pares de cobre y las centrales telefónicas definen la red de telecomunicaciones en ese imaginario colectivo.

Con la irrupción de las redes de datos, y de Internet hace más de treinta años, comenzó una profunda transformación de las tecnologías y la arquitectura de las redes de telecomunicación. Esta transformación se ha acelerado extraordinariamente en los últimos años con la irrupción de tecnologías como el 5G y la fibra. Estas tecnologías han acelerado también los procesos de transformación de la arquitectura de la red, con la "virtualización", la "cloudificación", y la "API-ficación" de las redes. Poco tiene que ver una red de telecomunicación desplegada en el año 2025 con esa imagen de la red de comunicaciones para la voz.

En paralelo a esta transformación tecnológica se ha acelerado también la transformación del sector de las telecomunicaciones. La liberalización de este sector en los años 90 del siglo pasado dio lugar a un sector diferente, con nuevos agentes, y diferentes tipos de operadores de telecomunicación: móviles, fijos, con red, virtuales, convergentes o especializados. Este sector, que se ha desarrollado a lo largo de las tres últimas décadas, está viviendo una implosión. La transformación ha dado lugar a un nuevo ecosistema de conectividad, en el que se está redefiniendo el papel de los operadores de telecomunicaciones dentro de una cadena de valor de la conectividad más amplia.

Los operadores coexisten ahora con grandes empresas tecnológicas, proveedores de servicios en la nube, empresas de infraestructuras (TowerCos, FibreCos, InfraCos), plataformas digitales y otros agentes clave que gestionan diferentes componentes de la infraestructura de conectividad. La creación de este ecosistema está definiendo el futuro de las telecomunicaciones.

El proceso está ocurriendo ahora, ante nuestros ojos. A lo largo de este capítulo abordaremos las causas, tecnológicas y de negocio, que han acelerado esta profunda transformación, la evolución del ecosistema de conectividad, y las implicaciones para el sector, y para la sociedad.

2.2. EL DESAFÍO DE LOS INGRESOS

De acuerdo con la asociación de operadores europeos Connect Europe (1), el crecimiento de los ingresos minoristas en el sector europeo de las telecomunicaciones se situó en el 1,7 % en el año 2023 (1). Una tasa de crecimiento que apenas ha variado respecto al año 2022, y que en términos reales (considerando la inflación) se redujo en un 4,4 %. La telefonía móvil, que representa algo más de la mitad de los ingresos, creció un 2,5 % y la fija un 0,9 %. Los ingresos del sector han descendido en términos reales desde el año 2016.

Si echamos la vista atrás algunos años más, podemos apreciar que la evolución de los ingresos de los operadores en Europa, comparada con la situación en otras regiones como Estados Unidos o Asia, muestra una situación mucho más desfavorable en el entorno europeo. Mientras en el período 2011-2022 los ingresos crecían un 18 % en Estados Unidos y un 12 % en Asia, en Europa los ingresos de los operadores de telecomunicación descendían un 33 %.

El sector de las telecomunicaciones ha sido un sector deflacionario en las dos últimas décadas. De acuerdo con Eurostat es el único sector económico en Europa cuyos precios siempre se han reducido en los últimos 20 años.

Esta presión sobre los precios es consecuencia directa del marco regulatorio de las telecomu-

nicaciones en Europa. La regulación diseñada para la liberalización del sector en los años 90 tenía como objetivo favorecer la entrada de nuevos operadores en el mercado, que pudiesen competir con los operadores incumbentes.

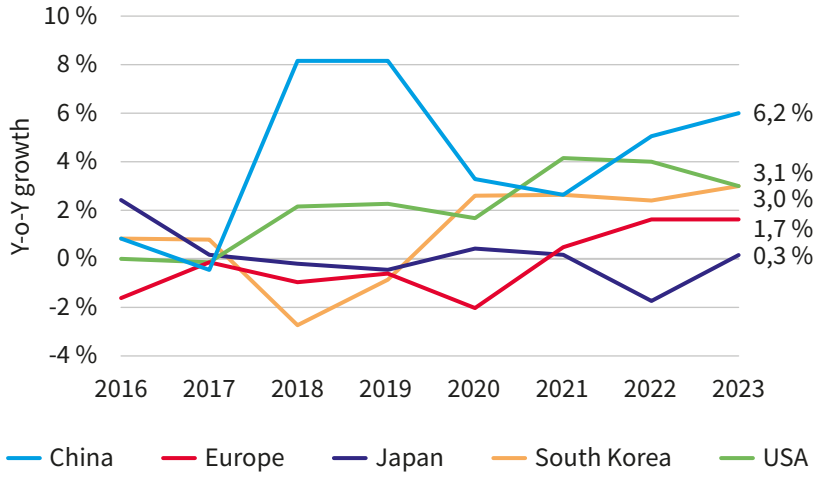


Figura 2.1.
Evolución ingresos sector Telco (var 2016/2023) (1).

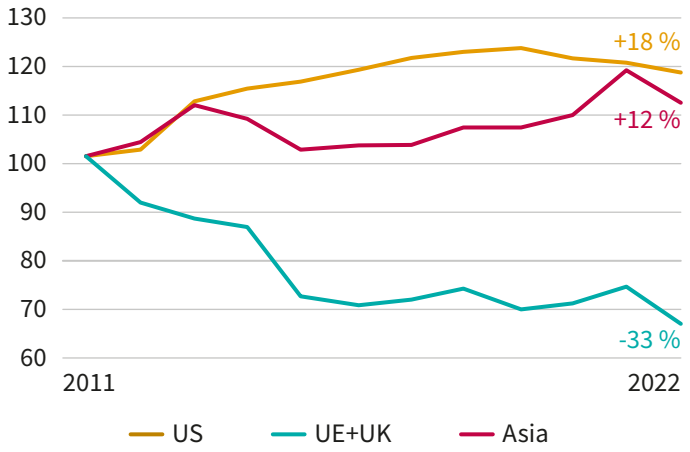


Figura 2.2.
Evolución ingresos sector Telco (Base 100-2011) (1).

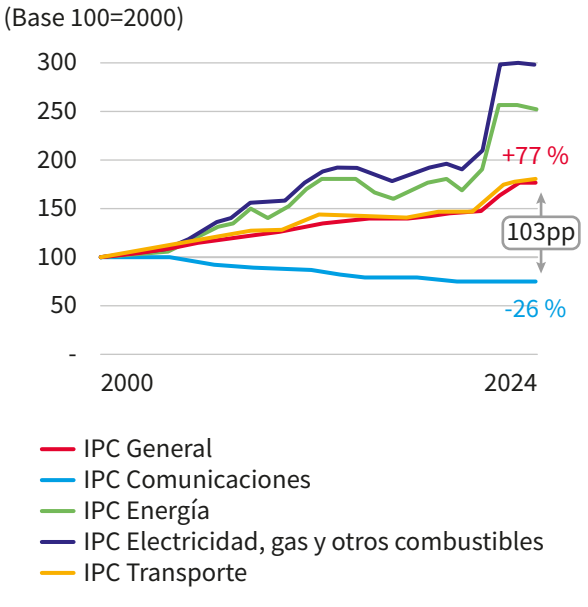


Figura 2.3.
Unión Europea evolución IPC: Presión deflacionaria desde décadas (2).

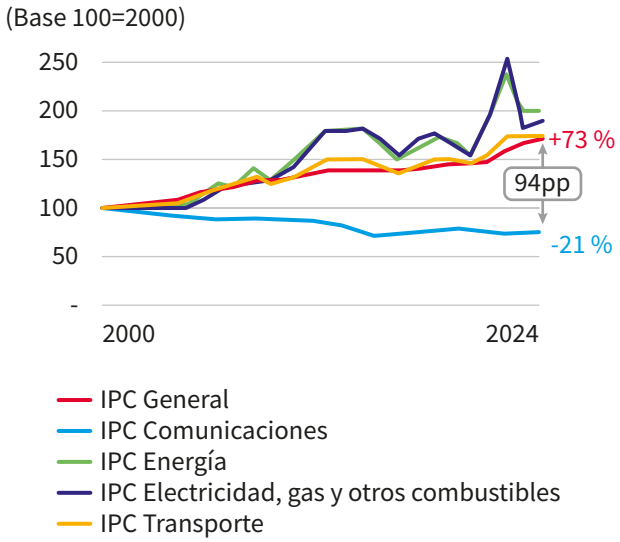


Figura 2.4.
España evolución IPC: Presión deflacionaria desde décadas (2).

Las sucesivas revisiones de este marco regulatorio han mantenido como objetivo la presión sobre los precios, impulsando una intensa competencia en el sector. La incorporación de la figura del operador móvil virtual en la primera década del siglo XXI reforzó esta presión regulatoria sobre los precios. Este modelo de operador no posee espectro, y carece de una red propia de acceso, por lo que su servicio se apoya en el uso de la red de otro operador con el que suscribe un acuerdo. Este modelo ha favorecido la fragmentación del mercado con la presencia de muchos operadores, lo que ha desembocado en una intensa competencia en precios y en un descenso de los ingresos.

Casi tres décadas después del inicio del proceso de liberalización, los operadores europeos afrontan numerosos desafíos ligados al descenso de la rentabilidad.

Desde el año 2017 la rentabilidad del capital empleado (ROCE - *Return on Capital Employed*) no ha dejado de descender, situándose por debajo del coste de capital (WACC - *Weighted Average Cost of Capital*).

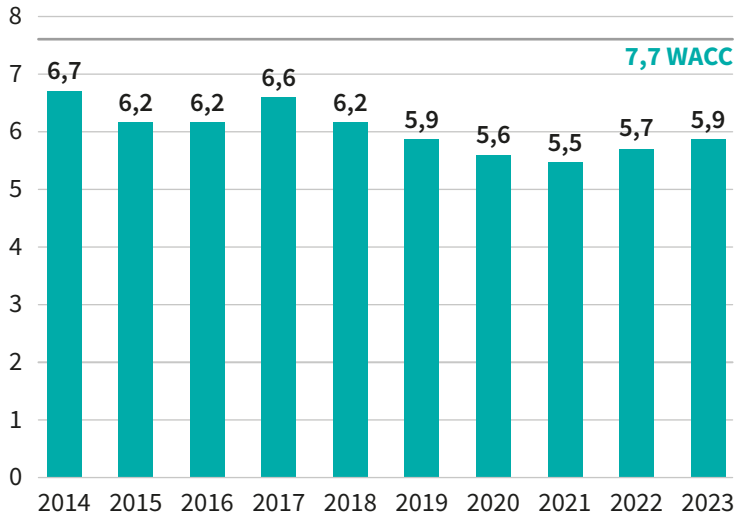


Figura 2.5.
Evolución del ROCE (1).

Este escenario ha reducido el atractivo para los inversores de los operadores de telecomunicación europeos, lo que se ha visto reflejado en un descenso en su valoración de mercado.

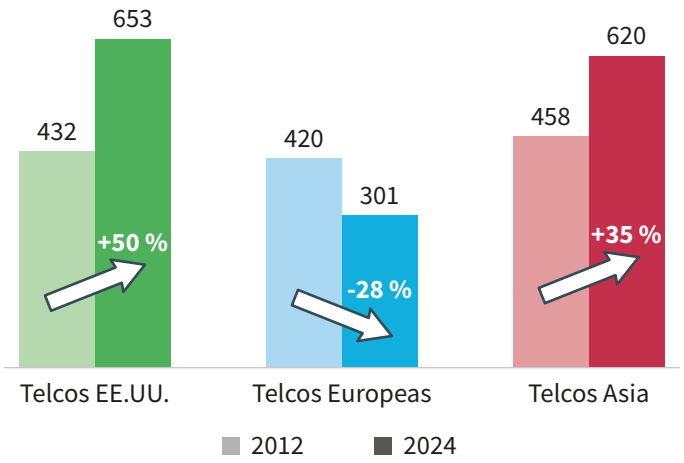
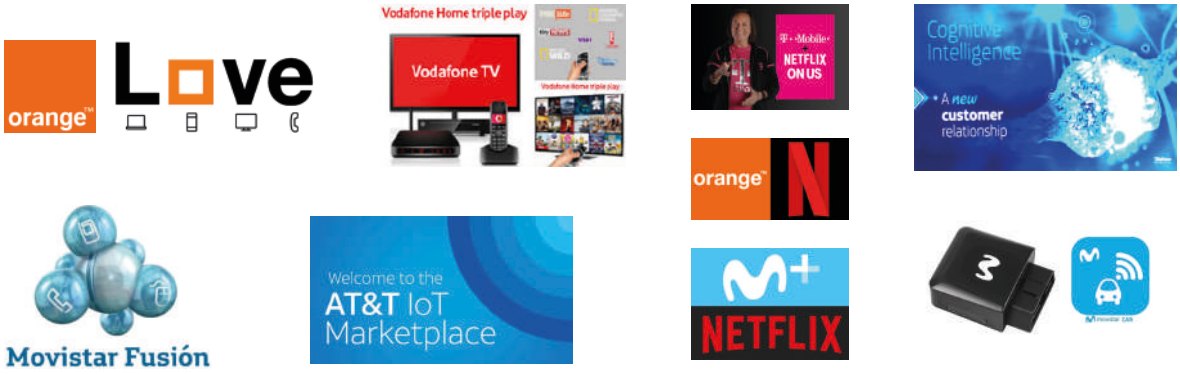
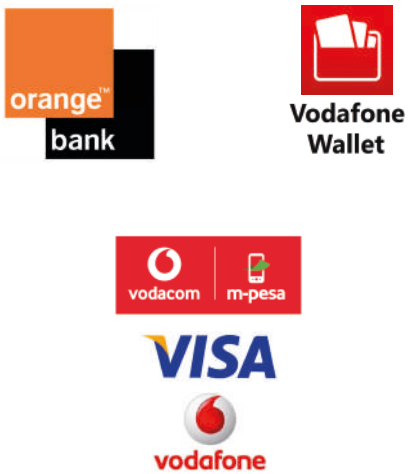


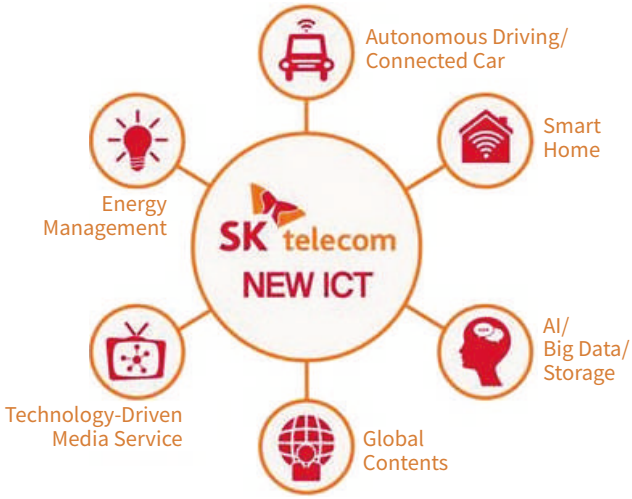
Figura 2.6.
Evolución capitalización bursátil de las Telcos (miles de mill, USD; %). Valor agregado de 4 Telcos EE. UU.; 13 Telcos Europa; 7 Telcos Asia (1).

En este contexto, el gran desafío para los operadores en los últimos años ha sido la búsqueda de nuevos ingresos. Mientras los ingresos generados por los servicios tradicionales de voz y banda ancha descendían, los operadores han intentado identificar nuevas fuentes de ingresos. La televisión, los contenidos, los servicios financieros, los servicios digitales, el IoT, la ciberseguridad, la IA, o la nube han sido algunos ejemplos de las estrategias de diversificación de los operadores.

En esta búsqueda de nuevos ingresos, la irrupción del 5G ha representado la gran oportunidad de materializar nuevas fuentes de ingresos.







2.3. LA EXPECTATIVA CREADA POR LA TECNOLOGÍA 5G

La tecnología móvil 5G ha supuesto una profunda transformación de las redes de telecomunicaciones, y ha creado a los operadores una expectativa de lograr nuevos ingresos. Respecto a las generaciones de tecnologías móviles anteriores, el 5G aporta mayor capacidad de ancho de banda y menor latencia. Esta mejora en las prestaciones de la tecnología móvil abre la puerta al desarrollo de nuevas aplicaciones y servicios que aprovechen estas características.

Los operadores han puesto gran parte de sus esperanzas para generar nuevos ingresos en las posibilidades de esta nueva tecnología.

2.3.1. Nuevos usos: banda ancha mejorada, IoT y baja latencia

La Unión Internacional de Telecomunicaciones (ITU) identifica tres grandes áreas de uso para la nueva tecnología 5G, con diferentes demandas de ancho de banda, latencia e inteligencia (3):

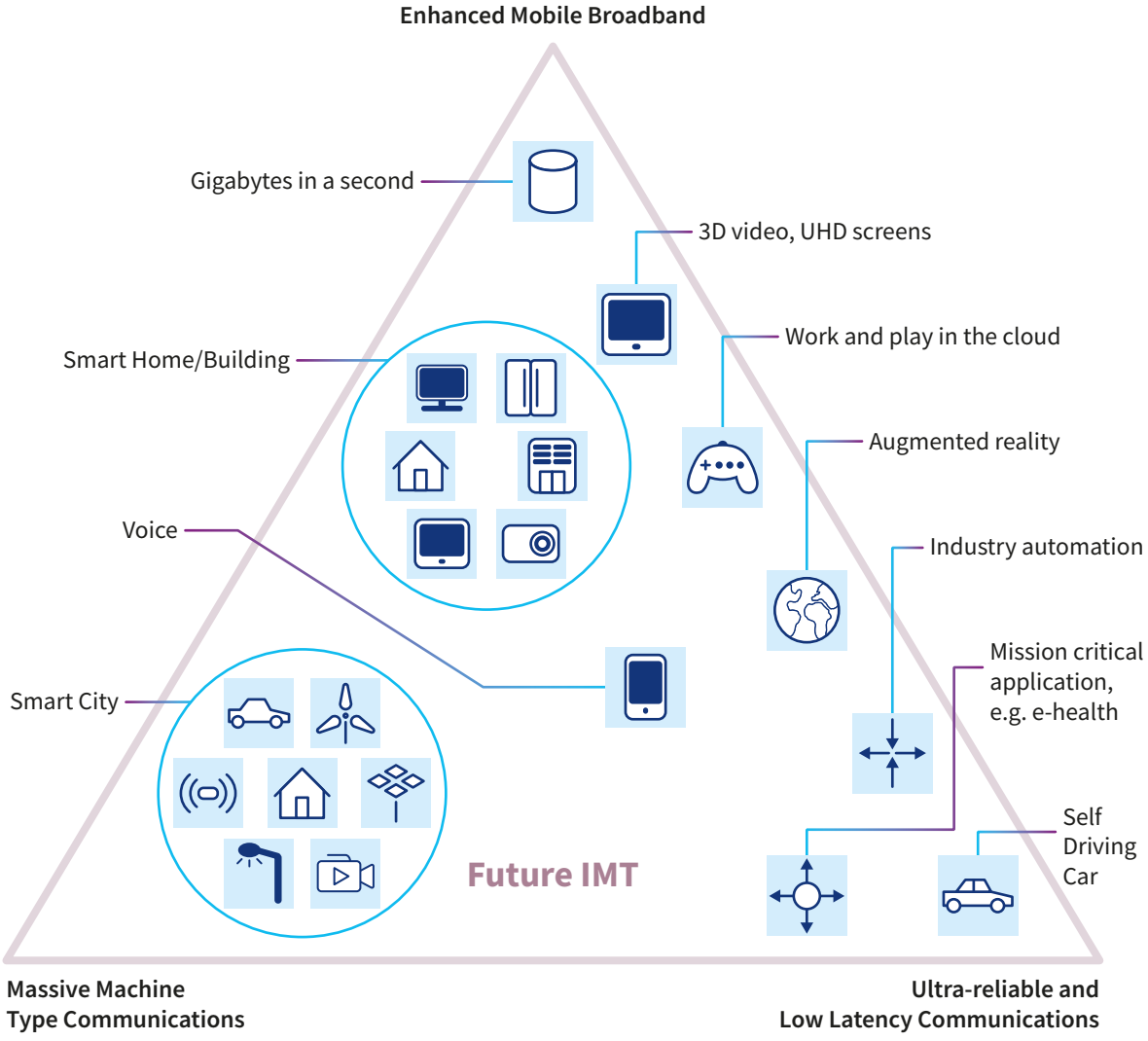


Figura 2.7.
5G Usage Scenarios (3).

- **Banda de ancha mejorada**: la mayor velocidad y capacidad que ofrece la tecnología 5G permite mejorar la experiencia de cliente, y ofrecer conexiones más rápidas que hagan posibles aplicaciones como la realidad virtual y la realidad aumentada.
- **Comunicación masiva entre todo tipo de dispositivos**: una red adaptada a las necesidades de las aplicaciones del IoT (internet de las cosas), como son la e-Salud, el transporte y la logística, las redes de energía inteligente, o la agricultura inteligente. El mundo *smart* hecho realidad.
- **Comunicación ultra fiable y de baja latencia**: una red para hacer realidad los vehículos autónomos, la gestión de drones o la industria 4.0.

Estas 3 grandes áreas de aplicaciones del 5G, y sus casos de uso asociados, proporcionan numerosas posibilidades para los operadores de poder materializar nuevos ingresos. GSMA, la asociación global de operadores móviles estima estos nuevos ingresos en 2,2 trillones (2,2 millones de millones) de dólares en los próximos 15 años (4).

2.3.2. Un servicio dirigido a las empresas y una materialización lenta

La realidad ha mostrado algunas dificultades para materializar estas expectativas. La tecnología 4G ofrecía una mejora sustancial en la experiencia de Internet en los dispositivos móviles. Para que los usuarios pudieran disfrutar de esta nueva tecnología y apreciar la nueva experiencia era suficiente con contar con un teléfono móvil equipado con la nueva tecnología. Se trataba de un servicio dirigido a las personas y de fácil acceso, ya que era suficiente con la compra de un nuevo terminal, y que aportaba un valor claro y apreciado por los clientes, que estaban dispuestos a pagar por él.

La tecnología 5G es una tecnología cuyas características aportan más valor a empresas. No es fácil que las mejoras de velocidad y capacidad que pueden percibir los usuarios con la nueva tecnología justifiquen un mayor gasto, y con él un incremento en los ingresos en el mercado del uso personal, por lo que el foco de las posibilidades de esta nueva tecnología se ha centrado en las empresas.

La posibilidad de materializar el desarrollo de la industria 4.0, o las posibilidades del IoT, han multiplicado el desarrollo de aplicaciones que hagan uso de las características de baja latencia y alta fiabilidad de esta nueva tecnología. Las fábricas de automóviles, los puertos, los entornos industriales, han sido algunas de las aplicaciones que han mostrado las posibilidades de esta nueva tecnología. El concepto de fábrica del futuro del fabricante de automóviles Mercedes-Benz en Alemania, conocida como *Factory 56* (5), mostró las posibilidades que la tecnología 5G podía aportar en estos entornos de fabricación. Fabricantes españoles como *Gestamp*, o fábricas en España como las de Seat en Martorell han desarrollado conceptos similares de fábricas del futuro, en las que el 5G juega un papel clave.

Aunque más lenta y compleja que la oferta asociada a la tecnología 4G, el desarrollo de las posibilidades asociadas al 5G no ha hecho más que empezar. Los casos de uso siguen multiplicándose en todos los entornos empresariales (6).

En el horizonte de medio plazo aparece la tecnología 6G, hoy en día asociada en gran medida a la incorporación de la inteligencia artificial en las redes, y a la posibilidad de hacer realidad las redes completamente autónomas. La tecnología probablemente no estará comercialmente disponible antes del 2035, y los operadores están actualmente centrados en materializar las verdaderas posibilidades de la tecnología 5G.

Hoy el 5G ya se ha convertido en uno de los principales habilitadores de la digitalización de las empresas en todos los sectores productivos, y una de las palancas claves de generación de nuevos ingresos de los operadores.

2.4. LA DECONSTRUCCIÓN DEL SECTOR: TOWERCO, FIBERCO E INFRACO

2.4.1. Empresas de torres (TowerCo)

En el verano del año 2019 la acción de Telefónica caía por debajo de los 6 euros. Como reacción a la caída de la acción, Telefónica presentó en noviembre de ese año un nuevo plan estratégico que entre otras acciones incluía la venta de 50.000 torres de telefonía móvil.

Este anuncio probablemente desveló para el gran público una tendencia que ya se había desarrollado en Estados Unidos, y que aceleraba su andadura en Europa: la venta de la infraestructura de torres y antenas de telefonía móvil de los operadores de telecomunicación, y la constitución de empresas de infraestructuras especializadas en estos activos, denominadas genéricamente "TowerCo".

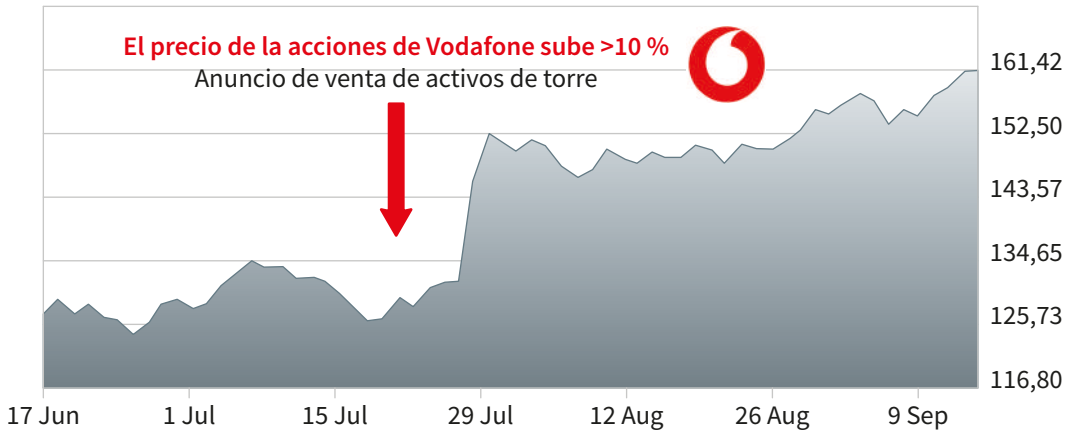
La razón tras estos movimientos es esencialmente financiera. La presión sobre los ingresos de los operadores, y las elevadas necesidades de inversión para el despliegue de nuevas tecnologías como el 5G y la fibra, ha empujado a los operadores a buscar nuevas fuentes de financiación mediante la venta de activos no estratégicos.

La mayoría de las torres donde se ubican las antenas no proporcionan ya una ventaja competitiva. En la etapa del 4G no ha sido ya habitual la competencia basada en la cobertura, por lo que la posesión de estos activos no se valora como estratégica.

En un escenario de tipos de interés bajos, los inversores buscaban alternativas de bajo riesgo para la inversión. Los fondos de infraestructura invirtieron inicialmente en autopistas, después en infraestructuras de energías renovables, y comenzaron a identificar a las infraestructuras de telecomunicación como un negocio atractivo.

Estas compañías de torres también tenían la capacidad de incrementar la eficiencia y rentabilidad en el uso de estos activos. Con la llegada del 5G se ha incrementado la densidad de las redes, con más torres y antenas, para poder proporcionar las prestaciones prometidas por esta nueva tecnología. Si la propiedad de las torres se encuentra en manos de una compañía diferente a los operadores, esta puede alquilarla a diferentes agentes, incrementando la eficiencia en su uso.

La conjunción de un período de tipos de interés bajos, la búsqueda de alternativas de inversión en infraestructuras por parte de los fondos, y la presión financiera provocada por la elevada deuda de los operadores, ha acelerado en los últimos años la venta de estos activos.



Vodafone realizó en el mismo período que Telefónica un anuncio similar. Solo el anuncio provocó el incremento en el precio de la acción de un 10 %.

La venta de las torres y antenas permitía a los operadores de telecomunicación cristalizar el valor de un activo, que en sus balances se encontraba infravalorado.

Entre las operaciones de este tipo realizadas en los últimos años, puede destacarse la venta de las torres de Telefónica al operador de infraestructuras americano American Tower. Telefónica vendió en enero del año 2021 su división de torres de telecomunicaciones en Europa (España y Alemania) y en Latinoamérica (Brasil, Perú, Chile y Argentina), por un importe de 7.700 millones de euros. El acuerdo establecía la venta de un número de, aproximadamente, 30.722 emplazamientos de torres de telecomunicaciones (7).

El precio que pagó American Tower era realmente atractivo, lo que revelaba el interés de esta empresa por incrementar su cartera de torres en Europa, y poder competir con su entonces principal competidor, la empresa española Cellnex. De acuerdo con las cifras proporcionadas por Telefónica, su negocio de torres había generado un beneficio en el año 2020 de aproximadamente 190 millones de euros. Considerando esta cifra, el múltiplo pagado por American Tower sería 30,5 veces el beneficio, lo que mostraba el atractivo del negocio de las infraestructuras de telecomunicación.

American Tower y Cellnex son dos de las principales empresas de infraestructuras TowerCo, creadas en este período. El negocio de estas empresas es más parecido a un negocio inmobiliario que al negocio de las telecomunicaciones, pero hoy en día forman ya parte esencial del ecosistema de conectividad, junto a los operadores de telecomunicación.

American Tower fue fundada en 1995, y es hoy uno de los mayores fondos de inversión inmobiliaria del mundo. Con presencia en 22 países, su cartera incluye cerca de 149.000 emplazamientos de comunicaciones, entre los que se incluyen más de 42.000 propiedades en Estados Unidos y Canadá y cerca de 107.000 propiedades a nivel internacional.

Por su parte **Cellnex** es el principal operador europeo de infraestructuras de telecomunicaciones móviles. Esta empresa transformó el negocio original de Abertis Telecom, centrado en la infraestructura de radiodifusión de la televisión digital terrestre, para convertirlo en un operador de infraestructuras centrado en las redes de nueva generación. Esta visión estratégica le ha permitido liderar este sector en Europa, con operaciones en 10 países, y con alrededor de 135.000 emplazamientos. A lo largo de los últimos años Cellnex ha realizado compras de torres en Francia, Italia, Suiza o Irlanda. Cellnex se ha convertido en una de las estrellas del mercado bursátil español, llegando a superar la cotización de Telefónica en el verano del 2020, como muestra del empuje y atractivo para los inversores de las empresas de infraestructuras de telecomunicación.

2.4.2. Empresas de Fibra (FiberCo)

Tras el éxito de las empresas de torres, se ha acelerado el desarrollo de empresas que invierten también en infraestructuras, pero en este caso en infraestructuras de fibra. Bajo la denominación de FiberCo se han multiplicado las operaciones dirigidas a acelerar el despliegue de fibra, basadas en el modelo de la creación de empresas de infraestructuras de fibra.

En este modelo, la FiberCo se constituye como un operador que comercializará la fibra como un servicio mayorista, dirigido a otros operadores de telecomunicación, que utilizarán esta infraestructura para dar servicio a los usuarios finales. Este modelo suele definirse como un **modelo de operadores neutros**, en el que las redes no estarían ya controladas por operadores de telecomunicación, sino que serían controladas por empresas especialistas en infraestructuras o por fondos de inversión en infraestructura.

El modelo de las FiberCo es un modelo más controvertido que el de las TowerCo, las empresas de torres. En este caso no todos los operadores comparten la visión de separar una infraestructura considerada estratégica como es la infraestructura de fibra, de la operación de un operador de telecomunicación.

En muchos casos este tipo de operaciones han respondido a una necesidad financiera. El alto coste del despliegue de fibra plantea unas necesidades de inversión que los operadores pueden encontrar difícil financiar ante las reticencias de los inversores. Para poder abordar estas inversiones, han explorado la creación de empresas separadas del operador, en las que han dado entrada a socios financieros. Los ejemplos recientes se han multiplicado en los últimos años.

Este es el caso de Telefónica en Alemania, con la creación de la empresa **UGG** (8), operador mayorista neutro de fibra, junto a la empresa de servicios financieros Allianz.

UGG es una empresa conjunta en la que Telefónica posee el 50 % y el 50 % restante *Allianz Capital Partners*. UGG anunció el objetivo de desplegar fibra para cubrir más de dos millones de hogares. El acuerdo se firmó en octubre de 2020 y las operaciones se iniciaron a principios de 2021. La empresa tiene previsto invertir hasta 5.000 millones de euros para abordar el despliegue de fibra en zonas rurales y semirrurales de Alemania.

Bluevía
Fibra de Telefónica

También en España Telefónica constituyó **Bluevía** (9) para desplegar fibra en zonas rurales. Bluevía es un operador de red que ofrece servicios mayoristas de acceso a fibra. Bluevía está participada por Telefónica y por los fondos de inversión Vauban y Crédit Agricole.

fiberpass

Recientemente, en febrero de 2025, Telefónica y Vodafone anunciaron la creación de **Fiberpass** una empresa conjunta en España para el despliegue de fibra, con el objetivo de alcanzar 3,6 millones de hogares. Esta empresa también daría entrada a otros socios financieros.

Ya en el año 2019, Más Móvil había vendido un millón de accesos de su red de fibra a un fondo de infraestructura por un importe de 217,5 millones de euros.

lyntia
NETWORK TO BUSINESS

En el panorama español de infraestructuras de fibra también destaca el operador **Lyntia** (10). Un operador neutro que cuenta con 55.200 km de fibra. Lyntia es propiedad de un consorcio empresarial formado por varios fondos de inversión: Axa IM Alts, Swiss Life Asset Managers y Morrison & Co.

2.4.3. Empresas de infraestructura (InfraCo)

Junto a las TowerCo, y a las FiberCo, también han surgido empresas de infraestructuras digitales generalistas denominadas InfraCo.

Telefónica creó en el año 2019 como parte de su nuevo plan estratégico la empresa **Telefónica Infra** (11), para agrupar activos de fibra, cables submarinos y centros de datos. En este caso, estas empresas responden a la agrupación de activos y la gestión de diferentes vehículos de inversión en infraestructuras de telecomunicación.

Las empresas de infraestructura de telecomunicación aparecen ya como una tendencia consolidada en el sector. Esta tendencia muestra que cada vez más partes de las redes de telecomunicación no serán propiedad de los operadores. Las redes serían controladas por especialistas en infraestructuras neutrales (Cellnex, Lyntia, …) o por fondos de infraestructura.

La tendencia a la desagregación del sector entre empresas de servicios y empresas de infraestructuras de telecomunicación sigue ganando terreno, configurando una profunda transformación en el sector.

2.5. EL IMPULSO TECNOLÓGICO: UNA NUEVA INFRAESTRUCTURA DE CONECTIVIDAD

2.5.1. Disrupción tecnológica

El panorama de las telecomunicaciones ha experimentado cambios sustanciales en los últimos años, tanto desde un punto de vista tecnológico, como en el número y tipo de empresas que participan, y en los modelos de negocio y de servicios que están surgiendo.

En gran medida estos cambios han sido impulsados por la innovación y la disrupción tecnológica. De la mano de la innovación tecnológica el sector de las telecomunicaciones avanza hacia una mayor virtualización de sus redes, hacia la integración de la nube en las redes, hacia una creciente presencia de las redes privadas y hacia un mayor uso de la inteligencia artificial (IA) en las operaciones de red (12) (13) (14).

Esta tendencia se ha visto impulsada por el despliegue de redes de alta capacidad, construidas sobre fibra y 5G, que junto con el Internet de las Cosas (IoT), los satélites de órbita baja, la computación en la nube y en los bordes (*Edge*), y la inteligencia artificial, están permitiendo crear una conectividad cada vez más inteligente, ubicua y flexible.

La Comisión Europea ha definido las nuevas redes como redes 3C (15): computacionales, colaborativas y conectadas. Estas redes integran capacidades informáticas que permiten el procesamiento en los bordes para reducir la latencia en aplicaciones sensibles al tiempo, como los vehículos autónomos. El aspecto colaborativo garantiza una interacción sin rupturas entre las diversas capas y actores del ecosistema, mientras que la dimensión conectada amplía la cobertura mediante la integración de redes terrestres y no terrestres (satelitales), creando una infraestructura digital más resiliente y eficiente. Abordaremos todos estos aspectos en este apartado.

2.5.2. 5G: virtualización y *softwarización* de las redes

La irrupción del 5G no solo ha supuesto una revolución en la gestión del espectro y el acceso radio con la utilización de la tecnología 5G New Radio o 5G NR, sino que también transforma el núcleo de la red.

Una red móvil tiene dos componentes principales: el núcleo, o *core* y el acceso radio. El núcleo de la red es el elemento que gestiona el tráfico de voz y datos, y las conexiones con las redes de otros operadores y con internet. La red de acceso radio se compone de los elementos que permiten la conexión con los usuarios, y comprende las torres, las antenas, y el equipamiento de radio, que hacen posible la conexión de los dispositivos móviles de los usuarios con la red.

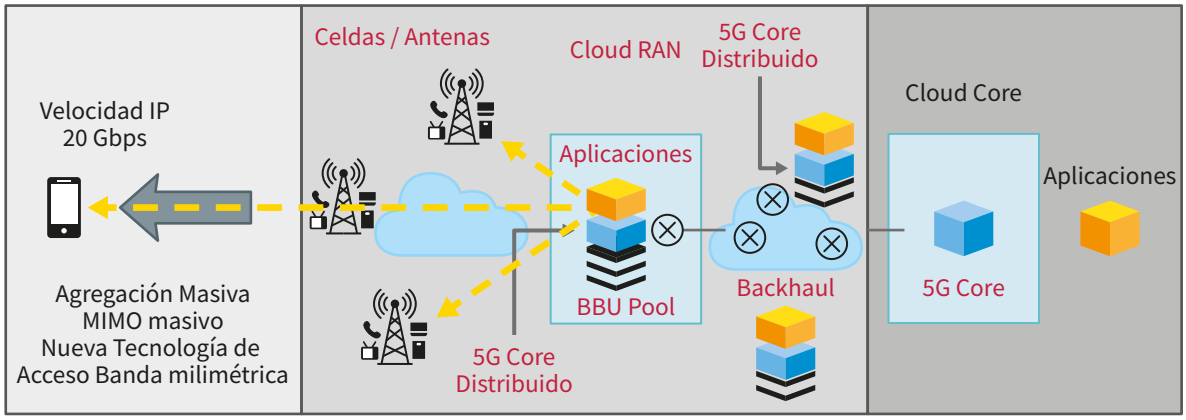
En la primera etapa del despliegue de las redes 5G, se compatibilizó la nueva radio 5G NR, con el núcleo de las redes 4G. Es lo que se ha denominado redes *5G Non Stand Alone* (5G NSA). Estas redes son hoy en día la mayor parte de las redes 5G desplegadas. Pero todo el potencial de la tecnología 5G se alcanza cuando a la nueva radio se le une el nuevo núcleo de red 5G. En este caso se trata de una nueva red en sí misma independiente de la 4G, una red *Stand Alone* (5G SA). Muchos operadores están ya desplegando estas nuevas redes 5G para poder aprovechar todas las capacidades que proporciona esta nueva tecnología.

El nuevo núcleo 5G impulsa un nuevo concepto de arquitectura de red, en el que muchas de las funciones se virtualizan y pasan a ser soportadas sobre una infraestructura de nube. Virtualizar la red implica que funciones que estaban soportadas en componentes específicos de la red como podían ser las antenas, los *routers*, o las centrales de conmutación, se convierten en un *software* que se ejecuta sobre una infraestructura de computación de propósito más general como es la nube.

A la desagregación del *hardware* y el *software* de los equipos de telecomunicación se le denomina "virtualización de la red". Este proceso facilita la actualización de las funcionalidades o la incorporación de nuevas características a la red sin tener que instalar nuevo *hardware*. Entre las muchas ventajas de esta nueva arquitectura de red cabe mencionar que cuando se trata de una modificación del *software* que no requiere la incorporación de nuevo *hardware*, las actualizaciones pueden realizarse simultáneamente en toda la red.

En esta nueva red, virtualización y *softwarización* caminan unidas para transformar las redes. En las nuevas redes 5G las funciones de red se convierten en aplicaciones que se ejecutan sobre la infraestructura de nube. Se habla entonces de la *Cloud RAN* que ejecuta funciones de la red de acceso, o de la *Cloud Core*, en la que se ejecutan las funciones del núcleo de la red.

Son muchas las implicaciones de este proceso de transformación de la red. Por un lado, parte del tradicional equipamiento de telecomunicaciones se convierte en *software*. El equipamiento de la red, como *routers* o centrales, evoluciona a aplicaciones *software*. Los proveedores de equipos de telecomunicación se convierten en proveedores de *software* y el *hardware* de la red se integra en la infraestructura de nube. El tratamiento de señal y el equipamiento de antenas se sigue manteniendo como equipamiento especializado, pero aun así el cambio en



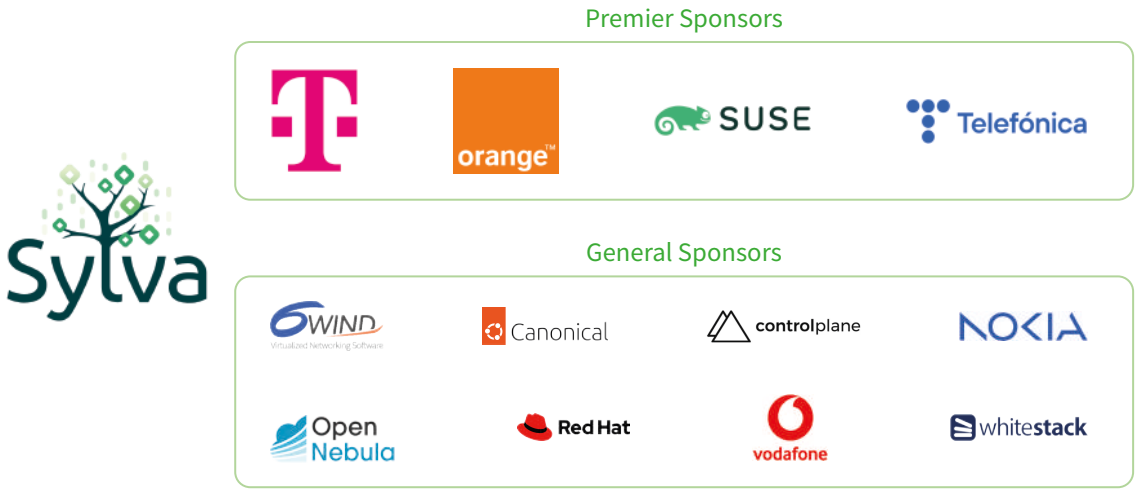
la arquitectura de la red tiene un profundo impacto en la infraestructura de conectividad.

Los proveedores de nube se convierten en proveedores de equipos e infraestructura clave para los operadores de telecomunicación. En esta tendencia, el sector de las telecomunicaciones también se mueve a la nube, como muchos otros sectores económicos. Estos proveedores de nube se convierten en competidores de los tradicionales proveedores de equipos de telecomunicación y en aliados clave de los operadores de telecomunicación.

En este escenario, los operadores de telecomunicación han iniciado diferentes proyectos para asegurar que la infraestructura de nube necesaria para la nueva infraestructura de conectividad se adecua a los especiales requisitos de las redes de telecomunicación. Cabe destacar el proyecto Sylva (16). En este proyecto los principales operadores de Europa, junto con los proveedores de equipos de red, se han unido para definir y crear una plataforma de nube que soporte los casos de uso específicos de los operadores de telecomunicación, como son la arquitectura 5G, el Open RAN o el Edge. Abordaremos estos casos y estas nuevas arquitecturas en apartados posteriores de este capítulo.

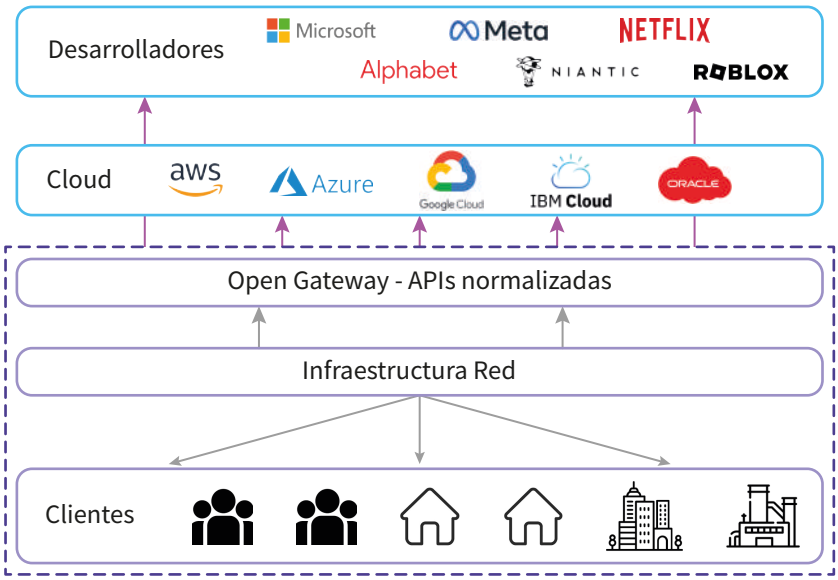
El proyecto Sylva, basado en un modelo de código abierto, aspira a crear la base de una infraestructura común entre los operadores europeos que permita la federación e integración de aplicaciones de Edge. El objetivo del proyecto es definir un marco de software en la nube adaptado a los requisitos de las infraestructuras de telecomunicaciones que aborde los retos técnicos de este ecosistema, así como desarrollar una implementación de referencia de este marco de software en la nube y crear un programa de validación para las diferentes implementaciones.

Este tipo de proyectos también pretende asegurar la compatibilidad e interoperabilidad de los diferentes proveedores de software de las nuevas redes. Estas iniciativas muestran la extraordinaria relevancia que los operadores de telecomunicación dan a esta nueva arquitectura de red soportada en la infraestructura de nube.



2.5.3. API-ficación de las redes: Open Gateway

Los operadores de telecomunicaciones están también adoptando modelos basados en la nube, como la red como servicio (NaaS) para virtualizar y mejorar su infraestructura. En ese intento de abrir las capacidades de las redes, y ofrecerlas como servicios a empresas y desarrolladores, los operadores han impulsado una iniciativa bajo el nombre de *Open Gateway* (17) en el marco de la asociación GSMA, que agrupa a todos los operadores móviles del mundo. De acuerdo con GSMA son ya 64 operadores móviles de todo el mundo los que se han unido



a esta iniciativa, lo que representa el 65 % de las conexiones móviles (18).

Esta iniciativa permite a los operadores exponer las capacidades de la red a través de APIs normalizadas, lo que hace posible que empresas y desarrolladores integren funciones avanzadas de conectividad directamente en sus aplicaciones. Una API es una interfaz de programación de aplicaciones, es decir es una interfaz normalizada que permite a las aplicaciones comunicarse entre sí para intercambiar datos o funcionalidades.

Tabla 2.1. Descripciones de APIs normalizadas (17).

Autenticación y prevención del fraude	Servicios de localización	Servicios de comunicación	Calidad de comunicación	Información de dispositivos	Servicios de computación	Pagos y cargos
Señal de desvío de llamada	Suscripción geolocalización		Perfiles de aplicaciones	Estado de accesibilidad del dispositivo	Descubrimiento sencillo del Edge	Facturación del operador
Rellenar conoce a tu cliente	Recuperación de localización		Información sobre conectividad	Suscripción estado de accesibilidad del dispositivo		Reembolso de facturación del operador
Coincidencia conoce a tu cliente	Verificación de localización		Suscripción información de conectividad	Estado roaming del dispositivo		
Verificación de número	Dato densidad de población		Calidad bajo demanda dispositivos del hogar	Suscripción a estado roaming del dispositivo		
Contraseña de un solo uso por SMS			Suministro Calidad bajo demanda			
Señal de estafa			Perfiles calidad de servicios			
Intercambio de SIM			Calidad bajo demanda			
Suscripción a intercambio de SIM			Información de sesión			

La apertura de APIs en las redes supone una disrupción tanto en la arquitectura de la red, como en los servicios que prestan los operadores de telecomunicación. El objetivo de *Open Gateway* es ayudar a los desarrolladores de aplicaciones y servicios, y a los proveedores de nube, a mejorar y desplegar servicios más rápidamente en las redes de los operadores a través de puntos de acceso únicos a la red.

Los APIs también ofrecen una visión uniforme de todas las redes de los operadores en todo el mundo, proporcionando acceso a una plataforma de conectividad que incorpora a todas las redes de telecomunicación. En la visión de los operadores, *Open Gateway* proporciona acceso a la mayor plataforma de computación que existe en el mundo.

La asociación GSMA estima que este modelo crea un nuevo mercado de 300.000 millones de dólares. Las APIs se estandarizan a través de la organización CAMARA (19). Esta organización se describe como un proyecto de código abierto dentro de la Fundación Linux para definir, desarrollar y probar APIs.

Hoy pueden ya encontrarse 27 APIs normalizadas que cubren áreas que abarcan desde la autentificación y prevención de fraude, servicios de localización, servicios de comunicación, calidad de la comunicación, información de dispositivo, servicios de computación y servicios de tarificación y pagos.

Open Gateway es una innovación disruptiva que aspira a transformar al sector y a los servicios de telecomunicaciones.

2.5.4. Open RAN: desagregación del acceso móvil

Open RAN es una iniciativa de infraestructura de interfaces abiertas en la red de acceso que los operadores móviles están desarrollando en el marco de la alianza O-RAN (O-RAN Alliance) (20). Esta iniciativa está relacionada con el proceso de virtualización y *softwarización* de las redes.

En las palabras de la alianza O-RAN, la iniciativa "se compromete a desarrollar redes de acceso por radio con inteligencia y apertura como principios fundamentales. Su objetivo es impulsar la industria móvil hacia un ecosistema de acceso radio (RAN) innovador, de múltiples proveedores, interoperables y autónomos, con un coste reducido, un rendimiento mejorado y una mayor agilidad" (21).

El objetivo de Open-RAN es desagregar el *hardware* y el *software* de las redes de acceso (virtualizar), de forma que puedan ser proporcionadas por diferentes suministradores.

No es extraño que esta iniciativa haya ganado impulso en un contexto en que en los últimos años se ha reducido notablemente el número de suministradores de equipamiento de telecomunicación tradicionales. A esta situación se unió las restricciones a los suministradores de equipamiento chinos y suministradores considerados de alto riesgo, impulsada por el gobierno de Estados Unidos. El reducido número de suministradores de equipos llevó a gobiernos como el de Estados Unidos o Japón a impulsar la iniciativa Open RAN, y a apoyar a los fabricantes que estaban desarrollando este modelo.

La iniciativa Open RAN precisa un proceso de estandarización, dado que, aunque tecnologías como el 4G y el 5G son estándares, no garantizan que los equipos de distintos suministradores puedan interoperar entre ellos. Habitualmente no son interoperables, lo que impide combinar equipos de diferentes suministradores en la misma red de acceso.

Open RAN nació para definir un conjunto común y abierto de interfaces para que las diferentes funciones de red virtualizadas (22) pudieran comunicarse. De este modo, las soluciones de los distintos suministradores pueden entenderse entre sí e interoperar. Además, esto posibilita que la función de red de un suministrador puede ser sustituida por la misma función de red de otro suministrador.

La iniciativa Open RAN supone desarrollar en el mundo de las telecomunicaciones el proceso que vivió el mundo de las Tecnologías de la Información en los años 80. El paso de soluciones cerradas y propietarias a estándares abiertos desagregó el camino del *hardware* y el *software* en el mundo de los ordenadores personales. Este proceso facilitó la aparición de nuevas empresas y nuevos servicios que impulsaron el desarrollo del sector de las tecnologías de la información.

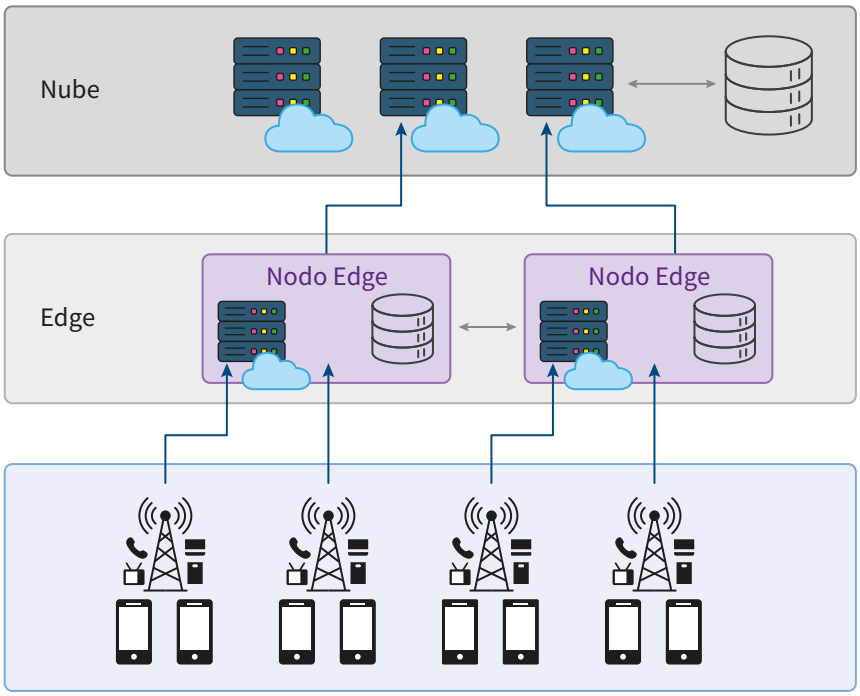
Bajo el impulso de la iniciativa Open RAN han surgido nuevos suministradores de equipos de telecomunicación, entre los que destacan Mavenir (23) y Rakuten (24). Los suministradores tradicionales, como Ericsson, Nokia, Samsung o NEC también se han sumado al desarrollo de este tipo de soluciones y arquitecturas.

El desarrollo de este modelo aún afronta desafíos en el ámbito de las prestaciones, la seguridad y la eficiencia energética, pero son ya numerosos los operadores que han abordado despliegues piloto de esta tecnología, especialmente en entornos de baja densidad de población.

2.5.5. Infraestructura de computación en el borde (*edge computing*)

Las redes de nueva generación desplegadas utilizando tecnologías 5G y fibra óptica proporcionan entre sus ventajas una menor latencia. La latencia es el tiempo en el que la información tarda en ir y volver del dispositivo del usuario a un servidor. Actualmente, el 4G ofrece de media unas latencias de 50 milisegundos. Con el 5G y la Fibra esa cifra puede bajar hasta 1 milisegundo. Para aprovechar las posibilidades que ofrece esta latencia reducida surge el *edge computing*, o computación en el borde (25).

El *edge computing* propone acercar la capacidad de procesamiento y almacenamiento a los usuarios, lo que reduce el tiempo de latencia, crítico en muchas de las nuevas aplicaciones que son posibles con las nuevas redes. Con la infraestructura de *edge* estamos acercando la nube al usuario, hasta el borde mismo (el *edge*) de la red.



Lo relevante en esta nueva infraestructura es que acercamos a los usuarios la capacidad de procesar y almacenar datos. Eso permite mover capacidades que antes estaban "lejos", en un servidor en la nube, mucho más cerca de los dispositivos.

El *edge computing* ofrece una alternativa más eficiente al escenario en que todos los datos se envían a la infraestructura de nube, más lejana. En el *edge* los datos se procesan y analizan más cerca del punto donde se crean, por lo que la latencia se reduce.

La reducción de latencia y la disponibilidad de capacidad de procesamiento y almacenamiento más cerca del usuario abre nuevas posibilidades a aplicaciones como el coche conectado o autónomo, la inteligencia artificial, la realidad aumentada o los videojuegos. Todas estas aplicaciones se benefician de una latencia reducida.

La infraestructura de computación en el borde ofrece una alternativa a las dos opciones de computación y almacenamiento disponibles actualmente: el procesamiento y almacenamiento en el dispositivo del usuario, o en la nube. Muchas aplicaciones buscan el equilibrio entre los requisitos en capacidad, procesamiento y consumo de batería cuando se realiza en los dispositivos del usuario, y la penalización en latencia cuando se realiza en la nube. Muchas aplicaciones pueden encontrar en el *edge* el equilibrio adecuado entre latencia reducida, y la reducción de los requisitos de procesamiento, almacenamiento y duración de la batería para los dispositivos de usuario.

Los operadores de telecomunicación cuentan con una infraestructura especialmente adecuada para el despliegue de la capacidad de computación en el borde. La ubicación de emplazamientos de antenas o las localizaciones donde se ubican las centrales telefónicas pueden albergar esta nueva infraestructura de *edge computing*.

Los operadores de telecomunicación han realizado algunos despliegues iniciales de esta nueva infraestructura en sus propias instalaciones. La infraestructura de computación en el borde puede entenderse como una extensión de la infraestructura de conectividad, aumentado su capacidad y la propuesta de valor que las redes de telecomunicación pueden ofrecer a sus usuarios.

2.5.6. Una red para la IA y una IA para la red

La inteligencia artificial (IA) es hoy en día la tecnología con mayor capacidad de disrupción en todos los ámbitos económicos y sociales. Las redes no pueden ser ajenas a esta nueva ola disruptiva.

Para la infraestructura de conectividad la inteligencia artificial presenta una doble perspectiva. Por un lado, las redes tienen que adaptarse para poder satisfacer las necesidades de los nuevos servicios basados en inteligencia artificial. Por otro lado, la incorporación de la inteligencia artificial en las redes promete un salto relevante en la capacidad de automatización en la gestión, y en la construcción de redes autónomas.

Las ventajas de implementar la tecnología de IA en las redes son cada vez más evidentes a medida que las redes se vuelven más complejas (26). La IA puede facilitar el mantenimiento y la operación de las redes. Podemos utilizar la IA para mejorar la resolución de problemas en las redes, acelerar la resolución de incidencias y proporcionar orientación para la reparación de averías o incidentes. La IA puede utilizarse para responder a los problemas en tiempo real, así como para mejorar el mantenimiento predictivo, anticipando los problemas antes de que se produzcan. También aumenta la información sobre seguridad al mejorar la respuesta y la mitigación de amenazas. Una de las áreas que ofrece perspectivas más prometedoras es la incorporación de la inteligencia artificial para mejorar la seguridad y resiliencia de las redes.

Las propuestas de trabajo sobre la tecnología 6G han identificado la IA como un elemento esencial en la definición de las nuevas redes. Es probable que la incorporación de las posibilidades de la inteligencia artificial en las redes de telecomunicación no espere a la aparición comercial de las redes 6G. Todos los fabricantes de equipamiento de telecomunicación están ya trabajando para incorporar esta tecnología en sus productos y servicios.

En otro ámbito, la explosión de aplicaciones y servicios relacionados con la Inteligencia Artificial tendrá un impacto en las redes que tendrán que adaptarse para hacer posible esta extraordinaria disrupción. El impacto más previsible es el incremento del tráfico, lo que requerirá una nueva inversión en capacidad por parte de los operadores de telecomunicación. Pero también se empiezan a observar otros impactos menos evidentes en los patrones de tráfico, como es el cambio en los patrones de tráfico de subida y bajada en este tipo de aplicaciones. Los diálogos propiciados por las aplicaciones de IA generativa y los nuevos servicios que la IA está haciendo posibles parecen requerir un patrón de tráfico de subida superior al que muestran otro tipo de aplicaciones.

Es fácil identificar que las aplicaciones de IA requieren una capacidad de procesamiento mayor que otro tipo de aplicaciones, pero suele pasar más desapercibido que en muchos casos también implican el intercambio de volúmenes masivos de datos, lo que tiene un claro impacto en las redes de telecomunicación.

En las aplicaciones de inteligencia artificial podemos identificar dos tipos de funcionamiento que dan lugar a cargas de procesamiento e intercambio de datos diferentes: el entrenamiento de modelos de IA, y el uso de estos modelos (27). El entrenamiento de una IA implica la recopilación de datos, la selección de modelos, el entrenamiento de los modelos y el despliegue de estos modelos. El uso de la IA implica desplegar el modelo entrenado para que pueda dar servicio a los usuarios y responder a sus entradas o consultas con una salida adecuada.

Para satisfacer todas estas necesidades de la inteligencia artificial, y las previsibles necesidades futuras, los centros de computación tendrán que conectarse mediante redes de alta velocidad, alta fiabilidad y baja latencia. La IA planteará nuevos requisitos a las redes de telecomunicación.

Aún estamos en un momento incipiente, pero la irrupción de esta nueva tecnología disruptiva obliga a los operadores a estar alerta para poder adaptar sus redes a los nuevos requisitos.

2.6. EL NUEVO ECOSISTEMA DE CONECTIVIDAD

2.6.1. Los operadores de telecomunicación ya no están solos

Como resultado de las nuevas dinámicas competitivas, la presión sobre la rentabilidad del sector, la disrupción propiciada por las nuevas tecnologías y las tendencias de deconstrucción, el sector de las telecomunicaciones se ha transformado en un **ecosistema de conectividad**.

La creación de este ecosistema implica que los operadores de telecomunicación ya no están solos. Ahora deben coexistir con otras empresas que también participan en este ecosistema, como son las grandes empresas tecnológicas, los proveedores de nube, las empresas de infraestructuras (TowerCos, FibreCos, InfraCos), las plataformas digitales y otros agentes clave que gestionan diferentes componentes de la infraestructura de conectividad.

El papel de las empresas de infraestructuras lo hemos ya abordado en un apartado anterior. En este apartado abordamos el resto de las tendencias que están reconfigurando el sector de las telecomunicaciones y creando el nuevo ecosistema de conectividad.

2.6.2. El papel de los proveedores de infraestructura de nube

Uno de los aspectos que tiene mayor trascendencia en la creación de este nuevo ecosistema de conectividad es la forma en que se están difuminando las fronteras entre la infraestructura de nube y la infraestructura de conectividad terrestre, a medida que la virtualización y la nube impulsan la convergencia tecnológica. Nube y conectividad configuran la nueva infraestructura digital.

Los grandes proveedores de servicios de nube cuentan con una infraestructura de centros

de datos y conectividad que rivaliza con la tradicional infraestructura de interconexión de las redes de telecomunicación, que solía denominarse el *backbone* internacional.

La extraordinaria escala de los grandes proveedores de nube como AWS, Microsoft o Google les permite contar con centros de datos y procesamiento distribuidos por todo el mundo, interconectados mediante redes privadas y cables submarinos.

Una parte relevante del flujo de tráfico internacional se realiza actualmente a través de las infraestructuras de nube de las grandes empresas tecnológicas.

Los proveedores de nube juegan por tanto un doble papel. Por un lado, cuentan con una infraestructura que proporciona conectividad, especialmente internacional, a los usuarios. Por otro lado, proporcionan un soporte básico para la nueva infraestructura de conectividad en su proceso de virtualización y cloudificación.

La infraestructura de nube se combina con la infraestructura de conectividad de los operadores en el nuevo ecosistema de conectividad para constituir la base de la nueva infraestructura digital.

2.6.3. Integración de redes terrestres y redes satelitales

La irrupción de los satélites de órbita baja, popularizados por el proveedor Starlink (28) ha ampliado el ecosistema de conectividad con nuevas posibilidades. Las comunicaciones móviles por satélite ofrecen la promesa de una cobertura ubicua en exteriores, complementando a las redes terrestres.

Los satélites de órbita baja proporcionan una mejora en la propuesta de conectividad, especialmente para zonas remotas o de baja densidad de población, y para servicios ligados al Internet de las Cosas (IoT).

Estos satélites también pueden prestar servicios a dispositivos móviles estándares, utilizando el espectro móvil, lo que suele denominarse servicio "directo al dispositivo" (D2D). Este es probablemente el salto tecnológico más innovador en la tecnología de satélite, y la que ha atraído más atención en los últimos meses.

Algunas compañías de satélites como AST SpaceMobile han anunciado recientemente que han podido completar con éxito en el año 2025 pruebas de videollamadas directas a dispositivos móviles con los operadores AT&T, Verizon y Vodafone (29) (30) (31). Starlink también ha anunciado que contará con capacidades y servicios directos al dispositivo móvil (D2D), como mensajería, datos e Internet de las cosas (IoT) y voz a partir de 2025 (32).

Algunos de los nuevos servicios de satélite a móvil van ligados a acuerdos con operadores de redes móviles. Estos acuerdos se están negociando a medida que las redes no terrestres y terrestres evolucionan, y las empresas comienzan a explorar posibles modelos de integración. Las empresas de satélites, como Starlink y AST SpaceMobile, han anunciado varios acuerdos con operadores de redes móviles en los últimos años (32) (33).

La conectividad proporcionada por los satélites de órbita baja puede complementar la cobertura de las redes móviles terrestres para todos los usuarios, que contarían con cobertura exterior universal. Esta conectividad también puede permitir nuevas aplicaciones en entornos aeronáuticos y marítimos, o la continuidad del servicio en situaciones como catástrofes naturales.

Aun cuando los servicios "directos al dispositivo" son aún un reto tecnológico, la nueva conectividad de satélite se posiciona como un complemento para las redes terrestres, y en algunos casos aspira a ser un servicio sustitutivo competitivo.

La coexistencia de conectividad basada en redes terrestres y en redes satelitales va a requerir reforzar la coordinación y cooperación entre estos agentes del nuevo ecosistema de conectividad, y resolver algunos retos tanto en el uso del espectro como en la interconexión.

2.6.4. El riesgo de desintermediación: e-SIM y *network slicing*

Las redes 5G incorporan una característica especialmente atractiva, las rodajas de red o *network slicing*. Esta característica permite la creación de múltiples redes lógicas sobre una infraestructura de red física compartida común ("redes virtuales aisladas" en 5G).

Esta capacidad ha comenzado a estar disponible en el año 2024, unida a los despliegues de 5G NSA y 5G SA por parte de los operadores. Aun cuando esta funcionalidad ya estaba disponible en la arquitectura *5G Non Stand Alone*, es con la nueva arquitectura *5G Stand Alone* cuando esta facilidad ofrece todas sus posibilidades. Las rodajas de red permiten la creación de redes virtuales extremo a extremo adaptadas a los requisitos de las diferentes aplicaciones.

Esta funcionalidad ofrece numerosas posibilidades con servicios adaptados a diferentes requisitos y clientes, pero también plantea un riesgo de desintermediación. La posibilidad de alquilar o contratar una de estas rodajas permitiría la entrada de otras empresas en el ecosistema móvil que no cuentan actualmente con acceso al espectro radioeléctrico.

Una situación similar se dio ya en el pasado reciente cuando algunos gobiernos plantearon la concesión de espectro a las grandes empresas de fabricación de automóviles, tal y como había hecho Corea del Sur, para garantizar su competitividad en el entorno de transformación de la industria 4.0.

Este modelo desintermediaba a los operadores de telecomunicación como proveedores de servicios de conectividad, dando entrada a otros agentes, muy en particular a los proveedores de equipamiento de red de esas fábricas que, utilizando este espectro, podían prestar directamente el servicio de conectividad a las fábricas sin la participación de los operadores.

Este riesgo de desintermediación no es el único que han afrontado los operadores en los últimos años. Probablemente el que despertó mayores recelos fue la creación de la eSIM o SIM virtual. La eSIM es una versión virtual de la clásica tarjeta SIM de datos.

La tarjeta SIM es el nexo entre un operador y su cliente. Esta tarjeta se instala en los dispositivos móviles e identifica el número de teléfono del usuario y el operador de telecomunicación. Un cambio de número o de operador requiere cambiar la tarjeta SIM.

La tarjeta SIM virtual fue impulsada inicialmente por los fabricantes de dispositivos que, en un entorno de restricciones de espacio en los dispositivos móviles, consideraban que a pesar de las sucesivas reducciones del tamaño de la tarjeta SIM, aún ocupaba un espacio muy preciado en los dispositivos. La necesidad se hizo más acuciante con la irrupción de nuevos dispositivos, aún más pequeños, que precisaban tarjetas SIM, como los relojes inteligentes.

Dado que la tarjeta SIM física situaba a los operadores de la red en el centro del ecosistema de conectividad móvil, su sustitución por la SIM virtual podría llevar a los consumidores a perder su último vínculo físico con los proveedores de servicios móviles. Esta pérdida de vinculación da una oportunidad de desintermediación a otros agentes, muy en particular a los fabricantes de dispositivos que cuentan con esa relación y ese vínculo con el comprador o usuario de sus terminales y dispositivos.

Los fabricantes pueden ambicionar vender no solo los dispositivos a los consumidores, sino también proporcionarles el servicio, convirtiéndose en operadores de redes móviles virtuales. En este escenario los operadores corren el riesgo de convertirse en meros proveedores de infraestructura en un modelo mayorista sin valor añadido, y sin relación con el usuario final.

Ninguna de estas amenazas de desintermediación se ha materializado actualmente. Pero sin duda plantean escenarios que podrían introducir cambios muy relevantes en el ecosistema de conectividad.

2.6.5. Un nuevo ecosistema de conectividad

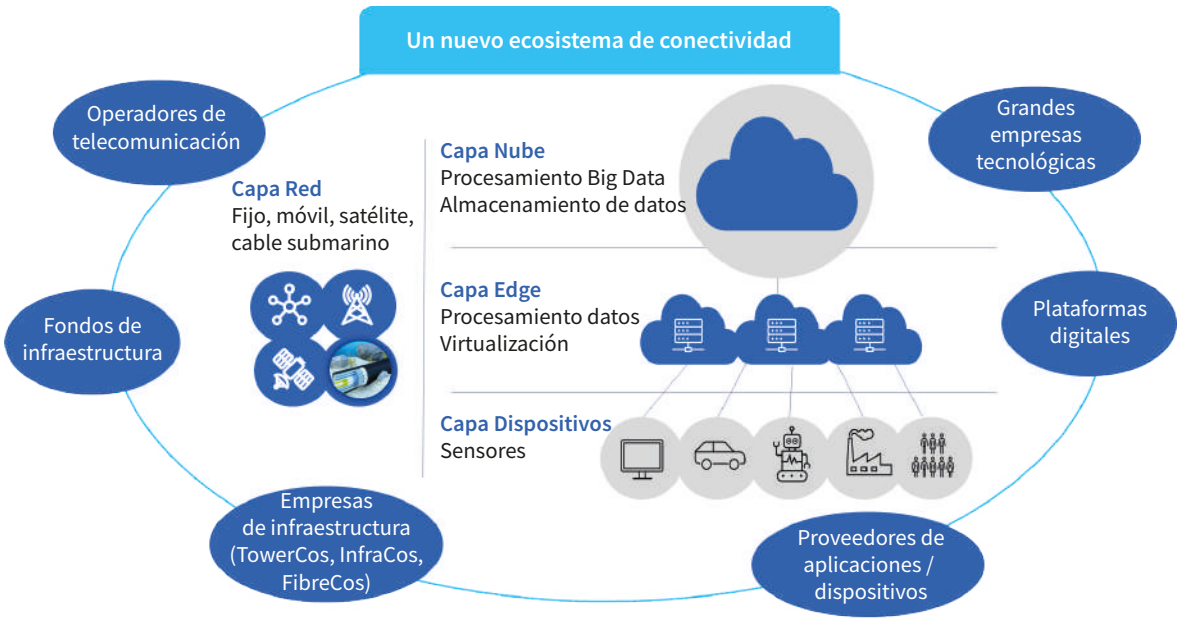
Todos los cambios descritos en los apartados anteriores muestran cómo operadores de telecomunicación y nuevos agentes coexisten en un nuevo ecosistema de la conectividad. En los apartados anteriores hemos visto cómo los proveedores de nube o los proveedores de satélite han entrado a formar parte de este nuevo ecosistema de conectividad, pero no son los únicos.

Si analizamos el ecosistema desde el punto de vista de la inversión, tal y como lo describía la OCDE en un informe reciente (34), las grandes empresas tecnológicas y los fondos de inversión han invertido también en diferentes capas de la infraestructura de conectividad.

Las grandes empresas tecnológicas están presentes en las redes de transporte a través de inversiones en cables submarinos y terrestres, así como en centros de datos, infraestructura en la nube y redes de distribución de contenidos (CDN). A menudo estas empresas colocan servidores de sus redes CDN directamente en la red de acceso de los operadores de telecomunicación.

Los fondos de inversión están igualmente presentes en varios segmentos, a través de inversiones realizadas en empresas de torres, centros de datos y empresas de fibra, tal y como describimos en el apartado sobre la deconstrucción del sector.

Todas estas dinámicas han dado lugar a un ecosistema de conectividad más complejo.



Este cambio está configurando un nuevo paradigma que requiere la colaboración entre las diferentes empresas que forman parte del ecosistema para impulsar la inversión, fomentar la innovación y mejorar la resiliencia.

Como elemento esencial de este ecosistema, los operadores de telecomunicaciones interconectan a varios actores y capas de infraestructura, incluidas las redes en la nube, las redes terrestres y las redes satelitales.

Un reto clave para la sostenibilidad a largo plazo del ecosistema de la conectividad reside en fomentar un entorno regulatorio y de políticas públicas en el que todos los actores puedan participar en los avances tecnológicos, innovar y desarrollar sus modelos de negocio. A medida que las infraestructuras en la nube, terrestres y no terrestres convergen para crear un nuevo ecosistema de conectividad, pueden surgir asimetrías regulatorias que provoquen desequi-

librios que socaven la competencia leal, los incentivos a la inversión y la eficiencia general del ecosistema.

Este reto definirá el futuro del ecosistema de conectividad. Abordamos cómo está afrontando Europa este reto en el siguiente apartado.

2.7. LA ADAPTACIÓN DE LA POLÍTICA DE TELECOMUNICACIONES EUROPEA

2.7.1. Un nuevo entorno precisa nuevas políticas

Con un sector en profunda transformación, un nuevo ecosistema de conectividad en el que coexisten diferentes empresas, y una completa transformación de la infraestructura de conectividad, es imprescindible abordar la adaptación del entorno regulatorio y de políticas públicas a esta nueva realidad.

Europa se encuentra inmersa en un proceso de revisión de sus políticas públicas con la competitividad y la innovación como grandes objetivos. Los informes elaborados por Enrico Letta (35) y Mario Draghi (36), publicados a finales del año 2024, han sido una clara llamada de atención a Europa para que aborde con urgencia el cierre de la brecha de innovación y productividad que amenaza su bienestar futuro.

El informe elaborado por Enrico Letta abordaba el desafío de completar el mercado único europeo. El sugerente título del informe, "Mucho más que un mercado", surge de la consideración del mercado único como una de las grandes palancas de competitividad y desarrollo económico de la Unión Europea. Por otro lado, el informe elaborado por Mario Draghi planteaba una perspectiva más amplia, y bajo el título de "El futuro de la competitividad europea" abordaba las barreras a la competitividad europea, y proponía diferentes acciones que deberían ponerse en marcha para cerrar las brechas de competitividad y productividad que lastran la economía europea.

A estos dos informes les siguió meses después la "Brújula de la competitividad" (37), publicada en enero de 2025 por la Comisión Europea. Esta brújula recogía la hoja de ruta para "restaurar el dinamismo de Europa, impulsar su crecimiento económico y lograr una Europa digital, descarbonizada, competitiva y resiliente que se afirme como líder mundial". La Brújula de la competitividad definía un plan de acción derivado de las propuestas realizadas por Mario Draghi y Enrico Letta en sus informes, centrado en tres ejes: cerrar la brecha de innovación, la estrategia conjunta para la descarbonización y la competitividad, y aumentar la seguridad y reducir las dependencias excesivas.

Todos estos informes reconocen al sector de las telecomunicaciones como un pilar estratégico clave de la competitividad europea, y por tanto como un agente clave en este objetivo de cerrar la brecha de competitividad e innovación. Las inversiones del sector son clave para sentar las bases de una economía digital competitiva soportada por una conectividad de alta calidad, segura y resiliente. La economía europea depende del acceso a redes de conectividad de alta capacidad para aprovechar todos los beneficios de la transformación digital.

Sin embargo, los informes de Draghi y Letta recogen también la necesidad de un nuevo marco regulatorio y de políticas públicas para abordar los retos actuales del sector. Los informes indican que para aprovechar el potencial del sector de las telecomunicaciones como pilar de competitividad, es esencial crear un entorno que garantice la sostenibilidad de sus inversiones.

A medida que evoluciona el ecosistema de conectividad, también es necesario un marco que se adapte a la nueva realidad. A medida que aumenta el número de empresas diferentes que participan en el ecosistema de

la conectividad, debe revisarse si el ámbito de competencia de los tradicionales reguladores de las telecomunicaciones abarca esta categoría más amplia de actores que forman parte del nuevo ecosistema de conectividad.

Por ejemplo, una cuestión relevante es el de las redes privadas. Como mencionamos en el apartado de las disrupciones en el ecosistema de conectividad, las grandes empresas tecnológicas poseen y operan diferentes infraestructuras de conectividad, que canalizan grandes cantidades de tráfico global. Una parte importante de ese tráfico se transmite a través de infraestructuras privadas, que conectan las infraestructuras de nube con los puntos de interconexión con los operadores de telecomunicación para llegar a los usuarios finales. Esto plantea cuestiones relativas al ámbito de aplicación de la regulación actual, ya que las redes privadas suelen estar fuera del mandato de los reguladores de las telecomunicaciones.

La cuestión del ámbito de aplicación de la normativa es igualmente necesaria en el contexto del papel creciente de las grandes empresas tecnológicas en el ecosistema de la conectividad. Son especialmente relevantes los proveedores de servicios en la nube y los proveedores de servicios digitales. A medida que crece el protagonismo de las grandes empresas tecnológicas en el ecosistema de conectividad, es imprescindible analizar si la nueva situación encaja en los marcos regulatorios actuales, y cómo deben adaptarse los marcos regulatorios para recoger adecuadamente esta nueva situación y asegurar un marco equilibrado que elimine las asimetrías regulatorias.

Igualmente, a medida que crece la inversión en infraestructura de comunicaciones por parte de las grandes empresas tecnológicas, las relaciones con los operadores de redes de comunicaciones se han modificado. Varias de estas grandes empresas tecnológicas son propietarias de cables submarinos, lo que los ha llevado a negociar acuerdos con los operadores, e incluso a arrendar capacidad a los operadores. Además, a medida que las grandes empresas tecnológicas poseen más infraestructura, cada vez más se asocian directamente con los operadores de telecomunicación para ubicar nodos de sus redes de distribución de contenidos (CDNs) en las redes de acceso de los operadores.

También las asociaciones y relaciones entre los operadores de redes de telecomunicación y los proveedores de nube se han incrementado y se han hecho más complejas. Es necesario también revisar la regulación actual para cuestionar si recoge adecuadamente la relación e interdependencia entre estos agentes.

Toda esta evidencia muestra que no es posible mantener el entorno regulatorio actual sin poner en riesgo la competitividad y sostenibilidad del sector, y de Europa. Un entorno regulatorio diseñado para la liberalización del sector de las telecomunicaciones hace más de 30 años, y centrado únicamente en los operadores de telecomunicación no puede responder a los desafíos que plantea la realidad de un nuevo ecosistema de conectividad.

2.7.2. La realidad actual del sector

La realidad actual del sector de las telecomunicaciones muestra una situación compleja. Como abordamos en el apartado dedicado al desafío de los ingresos, la reducción de los ingresos de los operadores europeos a lo largo de las dos últimas décadas ha puesto en riesgo la sostenibilidad y la capacidad de inversión del sector.

El descenso de los ingresos ha ido unido a un descenso en la rentabilidad. En la mayoría de los operadores europeos la rentabilidad ha estado por debajo del coste de capital en los últimos años. Esta situación ha tenido un claro impacto en la capacidad de inversión del sector. Mientras la inversión (CAPEX) per cápita en Estados Unidos es de 226,4€, en Europa se reduce a casi la mitad con 117,9€ (1).

Una menor inversión sostenida en el tiempo tiene un claro impacto en el despliegue de las nuevas redes y en los servicios y capacidades

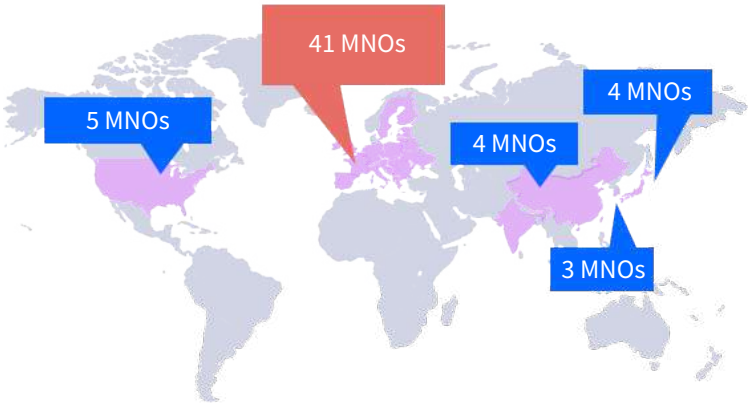
disponibles para los usuarios. Algunos datos muestran ya esta incómoda realidad.

De acuerdo con Connect Europe, en el año 2025 el despliegue de las redes 5G alcanzaba una cobertura en Europa del 87 %, mientras era del 98 % en Estados Unidos. Más diferencia se aprecia en el despliegue de 5G SA (*Stand Alone*), con un 2 % de cobertura en Europa, frente al 24 % en Estados Unidos a finales del 2024. Si nos fijamos en parámetros de prestaciones de las redes, la media de la velocidad de descarga en las redes fijas europeas es de 137Mbps, frente a los 246Mbps en Estados Unidos. En las redes móviles la situación es similar con 71Mbps en Europa frente a 108Mbsp en Estados Unidos. En el caso de las redes 5G SA compararíamos los 221Mbps en Europa frente a 384Mpbs en Estados Unidos (38). Estos datos muestran una realidad preocupante que pone en riesgo la competitividad europea.

Los operadores han planteado diferentes medidas necesarias para paliar esta situación. De acuerdo con los operadores, la excesiva regulación, la fragmentación del mercado y la baja rentabilidad del sector han provocado que Europa se quede atrás en desarrollo tecnológico y en innovación. Para paliar esta situación, los operadores plantean centrarse en cuatro objetivos:

1. **Escala**: el factor más relevante señalado por los operadores es la escala. Los operadores precisan alcanzar la escala necesaria en sus mercados para asegurar la rentabilidad de sus inversiones. Los operadores han señalado en repetidas ocasiones que no puede justificarse la existencia de más de 41 operadores con red en Europa, frente a los 5 en Estados Unidos, 4 en Japón, 3 en Corea del Sur o 4 en China (1). Hablamos de operadores con red y un número mínimo de usuarios, por lo que, si incluyéramos los operadores móviles virtuales o los operadores de nicho o regionales con un número reducido de usuarios, las diferencias serían aún mayores. Los operadores argumentan que no es justificable esta diferencia en el número de operadores, lo que tiene un claro efecto en la escala de los operadores europeos y en su rentabilidad y capacidad de inversión.
2. **Espectro**: el espectro tiene un gran impacto en el sector, tanto en la viabilidad de los servicios como en su rentabilidad, por lo que los operadores argumentan que es necesario promover una política de espectro alineada con los objetivos digitales.
3. **Simplificación regulatoria**: en la situación actual los operadores indican que es imprescindible eliminar y simplificar las barreras regulatorias para el despliegue de redes y la transformación del sector.
4. **Equilibrio en la cadena de valor**: los cambios en el ecosistema de conectividad plantean la necesidad de restablecer el equilibrio en el ecosistema, a través de marcos horizontales que eliminen los enfoques sectoriales y fomenten una relación justa entre los actores de la cadena de valor digital.

En este contexto, las políticas públicas y el entorno regulatorio desempeñan un papel clave para permitir al sector de las telecomunicaciones volver a la senda de la competitividad y la rentabilidad.



2.7.3. La respuesta europea: Libro Blanco de la Comisión Europea y la nueva regulación

En febrero del año 2024 la Comisión Europea publicó un Libro Blanco sobre las telecomunicaciones, con el título: *¿Cómo dominar las necesidades de infraestructura digital de Europa?* (15). La publicación vino acompañada de una consulta pública (39).

El Libro Blanco y la consulta pública prepararon el camino para la elaboración de una nueva ley de redes digitales (*Digital Network Act*) que debería adaptar el marco normativo europeo de las telecomunicaciones a la nueva realidad y al nuevo ecosistema de conectividad.

Este objetivo quedó recogido en el **Plan de trabajo de la nueva comisión europea** (40) publicado en febrero de 2025, donde se indicaba que la propuesta de la nueva ley debería estar lista en el último trimestre del 2025.

El Libro Blanco reconoce el valor estratégico del sector de las telecomunicaciones, y planteaba la necesidad de hacer más atractiva la inversión en redes abordando la baja rentabilidad, explorando nuevos modelos de financiación de las redes y resolviendo los retos en las áreas de espectro, innovación y despliegue de redes.

El documento también planteaba el objetivo de crear un verdadero mercado único europeo de las telecomunicaciones en el que los operadores alcanzaran la escala necesaria, superando la fragmentación.

El documento recoge los principales retos del sector que identificaba alrededor de tres áreas: tecnológicas, de escala y de seguridad.

En el ámbito de los desafíos ligados a la escala, el documento recoge varios retos: las necesidades de inversión, la compleja situación financiera, la ausencia de un mercado único europeo, la convergencia y la asimetría regulatoria (*level playing field*) y el reto de la sostenibilidad y la eficiencia energética.

El documento aborda por primera vez la necesidad de plantear un equilibrio entre la regulación de los operadores de telecomunicación y la regulación de los proveedores de infraestructura y servicios de nube, ante la evidencia de la creciente interrelación entre las dos infraestructuras. El documento plantea la pregunta sobre la conveniencia de aplicar la regulación de telecomunicaciones, en particular las reglas de acceso y resolución de disputas, a los proveedores de infraestructuras y servicios de nube. Esta pregunta reconoce abiertamente la creación de un nuevo ecosistema de conectividad que requiere una adaptación del marco regulatorio.

En el ámbito de la seguridad el Libro Blanco identifica el reto de los proveedores confiables, los estándares de seguridad, y la seguridad y resiliencia de los cables submarinos.

Para abordar estos retos, el documento propone varios escenarios alrededor de tres pilares:

1. **Crear las redes 3C**: Conectadas, Colaborativas y Computacionales.
2. **Completar el mercado único de las telecomunicaciones**.
3. Construir infraestructuras digitales **seguras y resistentes**.

En el marco de estos tres pilares el documento aborda políticas para el espectro, el apagado del cobre, el acceso a las redes de fibra, el servicio universal o la seguridad en la era de la computación cuántica, entre otras.

La **Ley de Redes Digitales** (DNA), entendida como el instrumento legislativo que debe definir el marco regulatorio y de políticas públicas para los próximos años, debería abordar los retos identificados en el sector y definir un nuevo marco para el futuro del sector de las telecomunicaciones.

Las expectativas alrededor de la nueva ley de redes digitales se han centrado en varios ámbitos, en línea con los retos identificados en el libro blanco:

1. **Favorecer la escala**: lograr escala es un requisito necesario para que los operadores de telecomunicación puedan recuperar

competitividad. Los operadores precisan un número suficiente de clientes (escala) en las áreas donde han desplegado las redes fijas y móviles. La política de control de fusiones en la Unión Europea ha limitado las posibilidades de consolidación de los operadores, con un claro impacto en su competitividad.

2. **Simplificar la regulación**: eliminar y simplificar las barreras regulatorias para el despliegue de redes y la transformación del sector.
3. **Impulsar políticas de espectro para fomentar la inversión**: los operadores esperan una mayor certidumbre jurídica y sostenibilidad financiera, con la ampliación de la duración de las licencias de uso del espectro, y con la definición de mejores prácticas en la concesión de licencias de espectro que eviten costes excesivos de espectro, y aseguren el acceso al espectro en frecuencias de banda media para satisfacer la demanda futura.
4. **Restaurar relaciones equilibradas** entre las diferentes empresas que forman parte del nuevo ecosistema de conectividad y de la cadena de valor digital. Este equilibrio debería permitir negociaciones equilibradas entre las diferentes empresas mediante la implementación de un mecanismo de resolución de disputas en los casos en que no sea posible un acuerdo comercial.
5. **Fomentar el nuevo ecosistema de conectividad**, definido por la relación **Telco-Cloud-Edge**, definiendo un marco común equilibrado para todos los actores y fomentando una mayor interoperabilidad e innovación.
6. **Apoyar la seguridad y resiliencia**: favorecer las inversiones necesarias en seguridad y resiliencia que debe afrontar el sector.

2.7.4. Un futuro por escribir

La Ley de Redes Digitales no es la única reforma legislativa que ha planteado la Comisión Europea para afrontar los restos de esta nueva etapa.

Todo el marco legislativo digital promulgado en la anterior legislatura europea debe coexistir con esta nueva ley. En este marco legislativo destacan la Ley de Servicios Digitales y la Ley de Mercados Digitales de la Unión Europea.

De cara al futuro, la Brújula de la Competitividad de la Unión Europea también establece acciones para desarrollar una Ley de Desarrollo de la Nube y la IA de la UE, una Ley del Espacio, junto a la Ley de Redes Digitales, entre otras, en los próximos uno o dos años (37).

Igualmente, la necesidad de ganar escala haría necesario la revisión de la política de competencia de la Unión Europea, y en particular de las "Directrices de concentraciones horizontales".

El momento es especialmente crítico para el sector de las telecomunicaciones europeo. Este nuevo impulso legislativo condicionará de forma decisiva el futuro del sector en la próxima década.

2.8. REFERENCIAS BIBLIOGRÁFICAS

1. Connect Europe (2025), "State of Digital Communications 2025". Disponible en: https://connecteurope.org/
2. Eurostat. Disponible en: https://ec.europa.eu/eurostat
3. ITU (2016). "Emerging Trends in 5G/IMT2020".
4. GSMA (2019). "The Mobile Economy 2019".
5. [Internet] https://group.mercedes-benz.com/innovation/production/factory-56.html

6. [Internet] https://www.telefonica.es/es/servicios/casos-de-uso-5g/

7. Telefónica (2021). Telefónica vende a múltiplos récord la división de torres de Telxius a American Towers por 7.700 millones de euros. Disponible en: https://www.telefonica.com/es/sala-comunicacion/prensa/telefonica-vende-a-multiplos-record-la-division-de-torres-de-telxius-a-american-towers-por-7-700-millones-de-euros/

8. [Internet] https://www.telefonica.com/es/t-infra/cartera/ugg/

9. [Internet] https://www.bluevia.es/

10. [Internet] https://www.lyntia.com/

11. [Internet] https://www.telefonica.com/es/t-infra/

12. Pier Luigi Parcu, Anna Renata Pisarkiewicz, Chiara Carrozza, Niccolò Innocenti (2023), "The future of 5G and beyond: Leadership, deployment and European policies", Telecommunications Policy, Volume 47, Issue 9, October 2023.

13. OECD (2022), "Broadband networks of the future", OECD Digital Economy Papers, No. 327, OECD Publishing, Paris.

14. OECD (2024), "OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust", Chapter 2, OECD Publishing, Paris.

15. European Commission (2024), "White Paper - How to master Europe's digital infrastructure needs?".

16. [Internet] https://sylvaproject.org/about-sylva/

17. [Internet] https://www.gsma.com/solutions-and-impact/gsma-open-gateway/

18. GSMA (2025). Which mobile operators are supporting Open Gateway? Disponible en: https://www.gsma.com/solutions-and-impact/gsma-open-gateway/which-mobile-operators-are-supporting-open-gateway/

19. [Internet] https://camaraproject.org/api-overview/

20. [Internet] https://www.o-ran.org/

21. [Internet] https://www.o-ran.org/what-we-do

22. Ericsson (2024), "What is Open RAN".

23. [Internet] https://www.mavenir.com/

24. [Internet] https://symphony.rakuten.com/open-ran

25. Blesson Varghese; Eyal de Lara; Aaron Yi Ding; Cheol-Ho Hong; Flavio Bonomi; Schahram Dustdar, (2021), "Revisiting the Arguments for Edge Computing Research", IEEE Internet Computing, Volume: 25, Issue: 5, October 2021.

26. CISCO (2025), "What Is Artificial Intelligence in Networking?".

27. Nokia (2024), "Networking for AI workloads".

28. [Internet] https://www.starlink.com/es

29. AT&T (2025). True Blue Connection: AT&T and AST SpaceMobile Take Connectivity to New Heights. Disponible en: https://about.att.com/story/2025/ast-spacemobile-video-call.html

30. Verizon (2025). Verizon completes its first satellite to cellular enabled video call with AST SpaceMobile BlueBird 2. Disponible en: https://www.verizon.com/about/news/verizon-ast-spacemobile-bluebird-2

31. Vodafone (2025). Vodafone makes world's first space video call from an area of no coverage using a standard mobile phone and commercial satellites built to offer a full mobile broadband experience. Disponible en: https://www.vodafone.com/news/technology/vodafone-makes-historic-satellite-video-call-from-a-smartphone

32. Starlink (2025). Starlink direct to cell. Disponible en: https://www.starlink.com/business/direct-to-cell

33. AST SpaceMobile (2025). Strategic Partners. Disponible en: https://ast-science.com/company/strategic-partners/

34. OECD (2024), "Financing broadband networks of the future", OECD Digital Economy Papers, No. 365, OECD Publishing, Paris.

35. Enrico Letta (2024), "Much more than a market".

36. Mario Draghi (2024), "The future of European competitiveness".

37. European Commission (2025), "A Competitiveness Compass for the EU".

38. Ookla's report (2025), "A Global Evaluation of Europe´s Digital Competitiveness in 5G Stand Alone".

39. European Commission (2025). Commission presents new initiatives for digital infrastructures of tomorrow. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_941

40. European Commission (2025). "Commission work programme 2025".

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

3

Evolución y tendencias del ecosistema digital global

Jorge Pérez Martínez

Pilar Rodríguez Pita

3.1. INTRODUCCIÓN

En las últimas décadas, el ecosistema digital está produciendo la acelerada transformación digital, a escala global, de la economía y la sociedad. Este entorno complejo y dinámico está compuesto por una amplia red de agentes, infraestructuras tecnológicas, plataformas digitales y marcos normativos que interactúan entre sí y evolucionan de forma interdependiente. Lejos de constituir un fenómeno estático, el ecosistema digital se caracteriza por su constante expansión, marcada por innovaciones disruptivas, cambios en los patrones de consumo de información, y la creciente centralidad de los datos como activo estratégico.

En este marco, resulta imprescindible adoptar una visión integradora del ecosistema digital que contemple tanto las infraestructuras tecnológicas subyacentes como los mercados y modelos de negocio que emergen de ellas. El concepto de ecosistema digital permite superar la tradicional dicotomía entre tecnologías y sectores económicos, al englobar de manera articulada los distintos niveles de la economía digital: desde el núcleo conformado por el sector TIC, hasta las plataformas digitales y la digitalización progresiva de sectores tradicionales. Este enfoque multidimensional permite comprender cómo la digitalización transforma no solo las herramientas de producción y comunicación, sino también las formas de organización empresarial, las cadenas de valor y los patrones de consumo.

El análisis de lo sucedido desde el año 2000 a nuestros días muestra cómo este ecosistema ha evolucionado hacia una estructura altamente compleja y globalizada, en la que conviven una creciente democratización del acceso a las tecnologías con fenómenos de concentración de poder sin precedentes. Empresas emergentes han logrado posicionarse como actores clave en menos de dos décadas, al mismo tiempo que un grupo reducido de gigantes tecnológicos domina vastas porciones del mercado digital. Este proceso ha sido acompañado por un notable incremento en la rentabilidad del sector, una atracción sostenida de inversiones en innovación y una transformación radical de las fronteras sectoriales. La comprensión de estas dinámicas es crucial para evaluar los desafíos económicos, sociales y regulatorios que plantea el ecosistema digital contemporáneo.

Desde hace unos años, las tensiones geopolíticas están condicionando su desarrollo. La reconfiguración hacia un mundo multipolar ha puesto en primer plano la disputa por el control de las infraestructuras críticas, el dominio de las redes de datos y la defensa de modelos regulatorios divergentes. Esta realidad subraya la urgencia de diseñar políticas de autonomía estratégica y marcos normativos que equilibren competitividad, protección de derechos digitales y resiliencia frente a riesgos de fragmentación tecnológica, un desafío especialmente acuciante para la Unión Europea en su búsqueda de un espacio digital soberano y cohesionado.

A partir de la clasificación de los países en arquetipos, ilustramos la amplitud de escenarios estratégicos disponibles para las economías digitales. Desde los núcleos de innovación que lideran la creación de tecnologías disruptivas hasta los consumidores sofisticados que constituyen mercados maduros de adopción rápida. Esta tipología no solo facilita la comprensión de las trayectorias históricas y estructurales de cada país, sino que también subraya la necesidad de diseñar hojas de ruta nacionales que fortalezcan las capacidades propias —investigación, talento, manufactura o servicios— y promuevan la movilidad gradual hacia eslabones de mayor valor añadido dentro del ecosistema global.

En este sentido, la Unión Europea enfrenta un doble reto: articular políticas colectivas que aprovechen sus altos niveles de inversión conjunta en I+D y sus marcos regulatorios avanzados (Reglamento de Inteligencia Artificial, Ley de Servicios Digitales, etc.), a la vez que reducen las desigualdades internas en infraestructura y capital humano. Iniciativas como Digital Europe y la Brújula de Competitividad ofrecen la plataforma para coordinar esfuerzos, pero su éxito dependerá de una gobernanza capaz de armonizar las prioridades sectoriales, optimizar la asignación de recursos y garantizar la interoperabilidad transfronteriza, cimentando así un verdadero mercado único digital.

3.2. EL ECOSISTEMA DIGITAL

3.2.1. Definición

Hay dos formas de aproximarse a las actividades económicas del ámbito digital, una es desde la propia articulación de las tecnologías y funcionalidades digitales, la otra es a partir de los mercados relevantes donde compiten los agentes del sector. En este apartado, proponemos una aproximación integradora que combina ambas perspectivas bajo el concepto de ecosistema digital.

Hasta finales del siglo XX, el ámbito digital estaba constituido exclusivamente por el sector de las Tecnologías de la Información y la Comunicación (TIC), que la OCDE definía en 1998 como una combinación de industrias manufactureras y de servicios que capturan, transmiten y muestran datos e información de manera electrónica (1). La llegada de Internet extiende el ámbito digital a nuevas actividades económicas susceptibles de realizarse de manera *online*, apareciendo el concepto de economía digital popularizado por Don Tapscott en 1995, uno de los primeros autores que mostraron cómo Internet cambiaría de modo radical la economía (2). En la actualidad, la economía digital se entrelaza de forma creciente con la economía tradicional (*offline*), lo que dificulta establecer una frontera clara entre ambas.

Como se ilustra en la **figura 3.1**, una posible solución a esta ambigüedad conceptual la presenta Bukht & Heeks (3), donde se propone describir el ámbito digital por tres términos: el sector de las TIC, la economía digital y la economía digitalizada. El sector de las TIC describiría la actividad económica relativa a la creación de infraestructuras digitales, el término de economía digital describiría los servicios digitales y la economía de las plataformas y, por último, bajo el término de economía digitalizada, abarcaríamos las actividades online del mundo *offline*. A continuación, se desarrollan estos conceptos:

- **El núcleo de la economía digital: el sector TIC**. Este segmento incluye componentes esenciales como los semiconductores, que son la base de todos los dispositivos electrónicos; el *hardware*, presente en toda la infraestructura digital y que abarca los componentes físicos y tangibles de los sistemas informáticos, de los dispositivos electrónicos y de las redes de telecomunicaciones; el *software*, conjunto de programas, protocolos y algoritmos intangibles que permiten controlar el funcionamiento de los sistemas electrónicos e informáticos; y los interfaces y dispositivos de usuario que permiten el acceso a los datos y contenidos digitales.

  También incluyen las infraestructuras que proporcionan la conectividad y la computación en la nube. Estas infraestructuras están compuestas por redes de alta velocidad como fibra óptica, redes móviles 4G y 5G, cables submarinos y satélites, etc.; los centros de datos que albergan servidores, sistemas de almacenamiento y equipos de red; las tecnologías de virtualización y contenedores que optimizan los recursos; y los servicios en la nube (IaaS, PaaS, SaaS) que ofrecen a sus usuarios capacidades escalables bajo demanda, como procesamiento, almacenamiento y aplicaciones accesibles desde cualquier lugar.
- **La economía digital**. Este segmento lo componen las funciones o aplicaciones digitales que crean valor económico añadido a los sectores empresariales y a los consumidores. Esto incluye servicios y plataformas (tanto B2C como B2B) que utilizan dispositivos e infraestructura de datos y conectividad como entradas. Estas plataformas son el núcleo de la economía digital y abarcan servicios como motores de búsqueda, sistemas de distribución de contenidos, generación automática de contenidos mediante IA generativa y redes sociales. Empresas como Google, Amazon, Facebook y Netflix son ejemplos paradigmáticos de este tipo de plataformas, que no solo facilitan el acceso a la información y los

bienes, sino que también generan nuevos modelos de negocio basados en la publicidad, la suscripción y la monetización de datos. Hablamos de una economía nacida en Internet, radicalmente innovadora y que continúa extendiéndose a todos los ámbitos de la actividad humana.

- **La economía digitalizada**. La digitalización ha dado lugar a nuevas actividades económicas y modelos de negocio que dependen en gran medida de las TIC. Entre ellos destacan el comercio electrónico, que ha transformado la forma en que las empresas venden sus productos a los consumidores y las plataformas *peer-to-peer* que facilitan la interacción directa entre usuarios, eliminando intermediarios y promoviendo la economía colaborativa. Ejemplos destacados incluyen a Amazon, Alibaba, Uber, Airbnb y TaskRabbit, que han revolucionado sectores como el comercio minorista, el transporte, el alojamiento y los servicios personales.

  En la actualidad toda la economía se está transformando digitalmente apareciendo, entre muchos otros, la industria 4.0, que integra tecnologías como el Internet de las Cosas (IoT), la robótica y la analítica de datos para optimizar los procesos industriales; la agricultura de precisión, que utiliza sensores, drones y sistemas de análisis para mejorar la eficiencia y sostenibilidad de la producción agrícola; el negocio electrónico que está transformando el sector bancario, etc. Estos avances no solo aumentan la productividad, sino que también abren nuevas oportunidades de innovación y crecimiento que generan empresas tecnológicas, ampliando el ámbito de la economía digital.

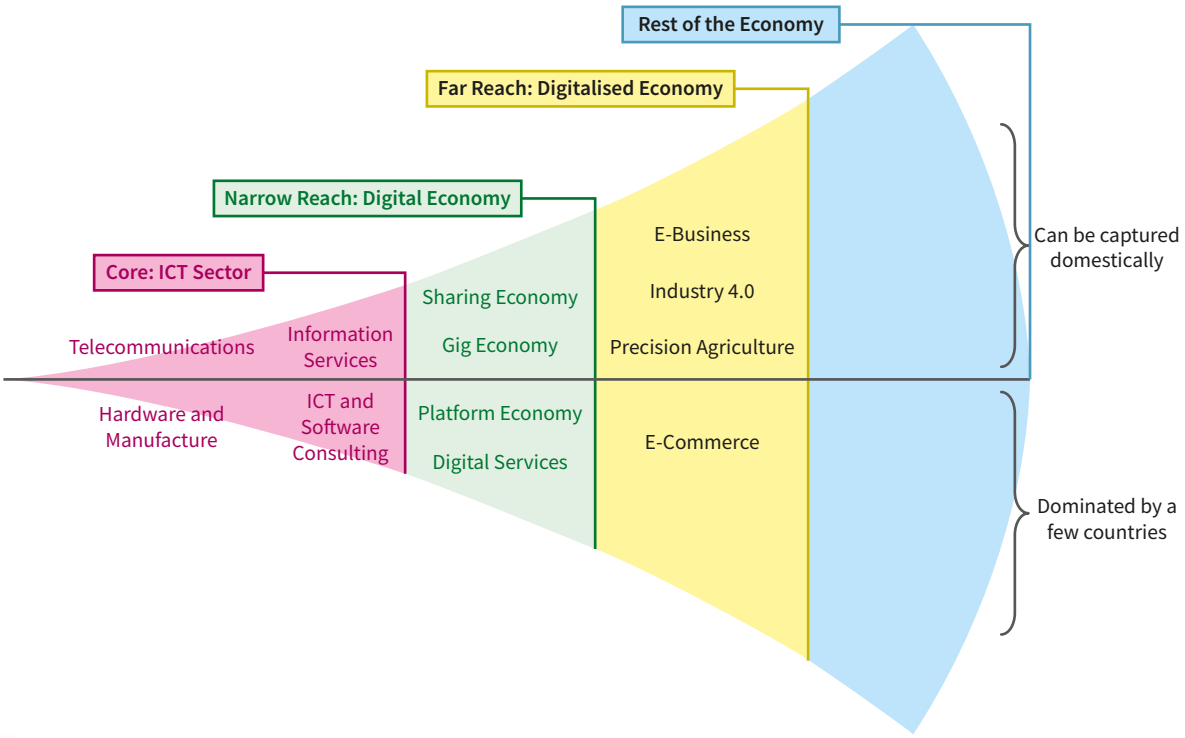


Figura 3.1.
La economía digital. Elaboración propia basada en (3).

En este trabajo hemos optado por englobar estos conceptos bajo una noción más integradora: el ecosistema o sector digital (4). En este ecosistema digital actúan un conjunto de agentes económicos diversos que, mediante la producción de dispositivos electrónicos, la construcción de infraestructuras y de plataformas tecnológicas sofisticadas, compiten y

cooperan para producir los bienes y servicios necesarios para la digitalización. Este ecosistema puede estructurarse en distintas capas funcionales: infraestructura, logística, plataformas y el internet abierto, aplicaciones, contenidos y usuarios (5).

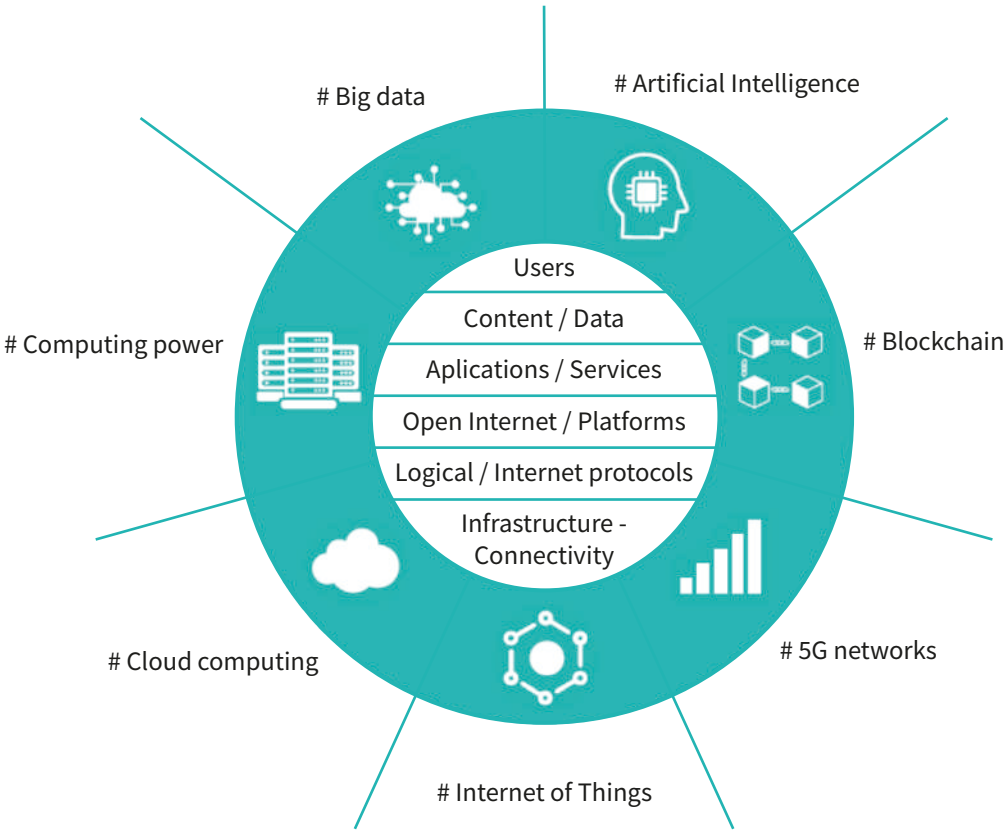


Figura 3.2.
Capas del ecosistema digital y sus habilitadores. Elaboración propia basada en (6).

3.2.2. Agentes principales del ecosistema digital

El ecosistema digital está compuesto por miles de empresas de muy diversa naturaleza y tamaño.

A partir de los datos sobre empresas cotizadas en bolsa, disponible en el portal CompaniesMarketCap.com[1], hemos elaborado la **tabla 3.1** donde podemos ver los principales agentes que operan en el sector digital, mostrando su posición en el *ranking* de las 100 mayores empresas del mundo según su capitalización bursátil, su valor, el país en el que tienen su sede y los segmentos industriales en los que operan (datos extraídos a mediados de abril de 2025).

1. CompaniesMarketCap.com es una plataforma en línea que ofrece información detallada y actualizada sobre la capitalización bursátil de empresas que cotizan en bolsa a nivel mundial. Actualmente, analiza un total de 10.507 compañías. Su función principal es clasificar a las compañías según su valor de mercado. Además del *ranking* general, el sitio proporciona datos financieros clave, el país de origen de cada empresa y otros indicadores relevantes para el análisis de mercado. También permite filtrar la información por países/regiones y por sectores industriales.

Tabla 3.1. Principales empresas del sector digital.

Rank	*Name*	*Marketcap*	*Country*	Sector TIC							Economía digital			Economía digitalizada	
				Semiconductores	*Hardware*	*Software*	IA	Electrónica	Operadores de telecomunicaciones	Computación de la nube	Internet	Entretenimiento	Videojuegos	Plataformas habilitadoras de servicios *peer to peer*	Comercio electrónico
1	Apple	2976,6	EE. UU.		X	X	X	X							
2	Microsoft	2887,6	EE. UU.				X			X			X		
3	Nvidia	2706,6	EE. UU.	X	X		X	X							
4	Amazon	1961,6	EE. UU.							X	X				X
5	Alphabet (Google)	1925,6	EE. UU.			X	X			X	X				
6	Meta Platforms (Facebook)	1377,6	EE. UU.				X				X				
7	Broadcom	855,5	EE. UU.	X											
10	TSMS	814,7	Taiwán	X	X										
17	Tencent	537,0	China							X	X		X		
21	Netflix	392,8	EE. UU.								X	X			
23	Oracle	371,1	EE. UU.			X	X			X					
29	SAP	302,3	Alemania			X									
31	T-Mobile US	295,3	EE. UU.						X						
37	Alibaba	266,8	China							X	X				X
38	ASML	263,0	Países Bajos	X	X										
39	Samsung	256,5	Corea del sur		X			X							
40	Salesforce	245,1	EE. UU.			X				X					
46	China Mobile	228,9	China						X						
48	Cisco	228,1	EE. UU.					X							
51	IBM	218,4	EE. UU.			X	X			X					
56	Palatir	207,7	EE. UU.			X	X								
63	AT&T	192,9	EE. UU.						X						
65	Verizon	187,6	EE. UU.						X						
77	Deutsche Telekom	169,8	Alemania						X						
79	Intuit	164,1	EE. UU.			X									
81	ServiceNow	162,6	EE. UU.			X					X				
87	QUALCOMM	154,0	EE. UU.	X	X										
92	AMD	151,7	EE. UU.	X	X			X							
93	Uber	151,2	EE. UU.								X			X	
94	Booking.com	150,5	EE. UU.								X			X	
95	Adobe	150,2	EE. UU.			X	X								
97	Xiaomi	150,2	China		X			X							
98	Sony	144,2	Japón		X			X				X	X		

La tabla muestra que siete empresas del sector digital encabezan el ranking y sitúa a 33 empresas entre las 100 más valoradas del mundo, que la mayor parte de ellas están radicadas en Estados Unidos o en países asiáticos y que se extienden por los distintos segmentos de la economía digital.

3.2.3. El ecosistema digital en la economía global

A partir del análisis de los datos de las 3.000 empresas más grandes del mundo desde 2005 hasta 2020, investigadores del McKinsey Global Institute (7), observaron que un número relativamente pequeño de industrias, casi todas pertenecientes al ecosistema digital, remodelaron la economía global. A continuación, mostramos en qué consistió esta remodelación:

- **Participación creciente en los beneficios de la economía global**. En 2005, el ecosistema digital representaba solo una pequeña fracción de los beneficios económicos globales. Sin embargo, para 2019, las empresas digitales representaban alrededor de la mitad de los beneficios económicos globales. Este crecimiento no solo refleja una expansión en el número de actores en el ecosistema, sino también el aumento de su rentabilidad. Este auge en los beneficios económicos ha sido impulsado por las altas tasas de adopción de tecnologías digitales y los modelos de negocio basados en plataformas, que permiten la explotación de grandes volúmenes de datos y una expansión sin precedentes de las redes.
- **Atracción de inversión para la innovación**. El ecosistema digital ha atraído, de manera significativa, inversiones en investigación y desarrollo (I+D) que alimentan su continuo crecimiento e innovación. Las empresas del ecosistema digital, como las que operan en la computación en la nube (Amazon Web Services, Microsoft Azure), la inteligencia artificial (Google AI, OpenAI) y la biotecnología digital (Illumina, Thermo Fisher), son grandes receptoras de estos fondos. Las inversiones no solo se destinan a la investigación básica, sino también a la creación de infraestructura digital global, plataformas de inteligencia artificial y tecnologías emergentes como el 5G, que prometen transformar la conectividad global.

  Además, el ecosistema digital ha generado incentivos para las empresas más grandes y consolidadas para realizar inversiones continuas en innovación para mantener su ventaja competitiva. En un mercado tan dinámico, donde nuevas tecnologías y modelos de negocio pueden reconfigurar rápidamente el panorama competitivo, las grandes empresas tecnológicas se ven obligadas a innovar de manera constante para no perder su liderazgo.
- **Entrada de Nuevos Competidores**. Una característica destacada del ecosistema digital es la facilidad con la que nuevos competidores pueden ingresar y desafiar a las empresas establecidas. A diferencia de industrias tradicionales, donde las barreras de entrada tienden a ser altas debido a los costos de infraestructura y la regulación, el ecosistema digital permite que startups e innovadores puedan competir eficazmente utilizando plataformas tecnológicas y modelos de negocio escalables.

  En 2020, aproximadamente el 34 % de la capitalización de mercado total del ecosistema digital estaba en manos de empresas que en 2005 no existían o eran actores irrelevantes.

  Este fenómeno de "nuevos jugadores" está impulsado por la naturaleza de las tecnologías digitales que permiten a las empresas escalar rápidamente a nivel global sin la necesidad de grandes inversiones iniciales en infraestructura física. Este fenómeno ha democratizado la competencia, permitiendo a empresas de todas las regiones y tamaños participar activamente en el ecosistema.
- **Alta concentración y presión por innovar**. Aunque el ecosistema digital ha fomen-

tado la entrada de nuevos competidores, también está marcado por una alta concentración de poder en manos de unos pocos actores clave. La concentración de la capitalización de mercado y los ingresos en unas pocas empresas ha sido significativa en ciertos sectores. Por ejemplo, los diez principales jugadores en áreas como la computación en la nube, la publicidad digital y los servicios financieros dominan el mercado global, representando más del 90 % de los ingresos y la capitalización de mercado en sus respectivos sectores.

Este fenómeno refleja la ventaja de las "economías de escala" en el entorno digital, donde los actores más grandes pueden reinvertir sus ingresos para mantener una ventaja competitiva, ampliando continuamente su infraestructura y capacidades. Además, la naturaleza de los efectos de red en el ecosistema digital fomenta la concentración, ya que el valor de las plataformas aumenta a medida que más usuarios se unen, lo que lleva a una mayor dominancia de las empresas líderes.

Sin embargo, esta concentración también crea una presión constante para innovar. Las plataformas dominantes deben invertir de manera continua en I+D, nuevas características de productos y expansión de mercados para mantener su competitividad. De lo contrario, los nuevos competidores o las tecnologías disruptivas pueden desplazar rápidamente a los líderes establecidos.

- **Alcance global**. El ecosistema digital tiene un alcance global sin precedentes. La conectividad a Internet, la adopción de dispositivos móviles y la digitalización de los servicios han creado mercados internacionales donde los actores digitales pueden operar en múltiples países y regiones al mismo tiempo. Se estima que el 50 % de los ingresos generados por las empresas digitales provienen de fuera de sus países de origen, destacando la capacidad de las empresas tecnológicas para escalar a nivel mundial.

  Las plataformas que controlan la publicidad digital como Google, las plataformas de comercio electrónico como Amazon y Alibaba, los servicios de transmisión de video como Netflix y Spotify, y las plataformas de redes sociales como Facebook y Twitter operan en múltiples países y continentes, ajustando sus modelos de negocio a las necesidades y preferencias locales, pero manteniendo una estructura global.

  Este alcance global ha sido posible gracias a la infraestructura digital, que permite la distribución de productos y servicios a nivel mundial sin las restricciones de las fronteras físicas. Además, las políticas y regulaciones locales han tenido que adaptarse a esta nueva realidad, creando desafíos tanto para las empresas como para los gobiernos.

- **Generación de gigantes globales**. El ecosistema digital ha dado lugar a una nueva clase de gigantes globales, empresas que, debido a su modelo de negocio escalable y su capacidad para aprovechar las redes globales, han crecido a un ritmo sin precedentes. Estas empresas incluyen nombres como Amazon, Apple, Microsoft, Google, Facebook y Alibaba, que han acumulado miles de millones de usuarios y tienen una presencia global.

  En 2020, el 74 % de la capitalización de mercado de las empresas digitales estaba en manos de compañías con una capitalización de mercado superior a $50 mil millones, y el 49 % de estas empresas superaban los $200 mil millones en capitalización. En comparación, las industrias tradicionales, como la manufactura o la minería, tienen una representación mucho menor de empresas de este tamaño.

  Estos gigantes globales han sido impulsados por el modelo de negocio de plataformas tecnológicas, que permite la explotación de redes de usuarios, datos y servicios sin necesidad de una infraestructura tradicional costosa. Empresas como Amazon, que comenzó como un minorista en línea, ahora domina el comercio electrónico global, el almacenamiento en la nube y los servicios de transmisión de video. Google, que comenzó como un motor de búsqueda, ahora es líder en publicidad digital, inteligencia artificial y sistemas operativos móviles.

A partir de los datos sobre empresas cotizadas en bolsa, disponible en el portal CompaniesMarketCap.com, hemos elaborado la **tabla 3.2** a partir de datos extraídos a mediados de abril de 2025 del portal CompaniesMarketCap.com, donde mostramos algunos indicadores sencillos que muestran la situación actual del sector digital en el conjunto de la economía global.

Entre las 10.436 de mayor capitalización bursátil el ecosistema digital sitúa 1000 empresas que representan el 10,5 % de las empresas, el 10,6 % de los ingresos y el 9,8 % de los empleos, es decir el 10 % de la economía total. Sin embargo, representan el 15,1 % de los beneficios y el 26,2 % de la capitalización.

Por otro lado, puede observarse que dentro del ecosistema digital las categorías *software* e Internet capturan mucho más valor que las demás y que las 58 empresas que actúan en la categoría de "inteligencia artificial" capturan un valor enorme de la capitalización total.

Tabla 3.2. La captura de la economía global por el sector digital.

Categoría	Número de empresas	% sobre el total de empresas	Capitalización bursátil (en trillones americanos)	% capitalización bursátil sobre el total	Ingresos (en trillones americanos)	% sobre el total de ingresos	Beneficios (en trillones americanos)	% beneficios sobre el total	Empleo (millones)	Empleo sobre el total
Total	10.436	100 %	107,265	100 %	57,73	100 %	7,381	100 %	128967715	100 %
Grandes empresas tecnológicas	1.092	10,5 %	28,098	26,2 %	6,141	10,6 %	1,116	15,1 %	11440380	8,9 %
Telecomunicaciones	205	2,0 %	3,123	2,9 %	2,122	3,7 %	0,2392	3,2 %	4324249	3,4 %
Semiconductores	135	1,3 %	6,524	6,1 %	1,056	1,8 %	0,27122	3,7 %	1166227	0,9 %
Software	501	4,8 %	12,265	11,4 %	1,763	3,1 %	0,45441	6,2 %	3326630	2,6 %
Comercio electrónico	103	1,0 %	3,023	2,8 %	1,275	2,2 %	0,13488	1,8 %	2919533	2,3 %
Internet	315	3,0 %	9,158	8,5 %	2,415	4,2 %	0,42231	5,7 %	4251661	3,3 %
Videojuegos	234	2,2 %	4,028	3,8 %	0,60065	1,0 %	0,16346	2,2 %	855309	0,7 %
IA	58	0,6 %	13,076	12,2 %						

3.3. LA CONSTRUCCIÓN DEL ECOSISTEMA DIGITAL GLOBAL 2000-2017

Desde sus inicios, generalmente asociados con el surgimiento de Internet en la última década del siglo XX, y hasta la llegada de Donald Trump a la presidencia de Estados Unidos en 2017, la evolución del ecosistema digital global ha estado marcada por dos fenómenos fundamentales: la revolución tecnológica y el proceso de globalización. A medida que se producían sucesivas disrupciones tecnológicas, los países integraban nuevos productos y servicios de las tecnologías de la información y la comunicación (TIC), lo que impulsaba la transformación digital de diversos sectores económicos, así como la modificación de los hábitos y costumbres de la ciudadanía, en un proceso conocido como digitalización. Paralelamente, la globalización favoreció el desarrollo de sectores digitales nacionales, interdependientes orientados a satisfacer tanto las demandas de los mercados locales como las del mercado global. Este proceso derivó en una especialización económica en la que cada nación ha acabado

ocupando un lugar específico en alguno de los eslabones de la cadena de valor global.

Este fenómeno no hubiera sido posible sin el contexto de confianza vivido entre el año 2000 y el año 2017, donde las relaciones económicas internacionales se desarrollaban en gran medida al margen de tensiones geopolíticas significativas. En efecto, durante este período el comercio de bienes y servicios, la circulación de capitales, la localización de inversiones productivas y la transferencia de tecnología se consolidaron como dinámicas transfronterizas. El mundo asumió que solo EE. UU. poseía la capacidad de garantizar las condiciones de seguridad y confianza necesarias para desacoplar las relaciones económicas internacionales de las inevitables tensiones geopolíticas que aparecían entre países con regímenes políticos, niveles de desarrollo económico y culturas profundamente divergentes. En este contexto, conceptos como la autonomía estratégica, la soberanía tecnológica y el control de las cadenas de suministro se vincularon casi exclusivamente al ámbito de la seguridad y la defensa, sin influir de manera significativa en las políticas económicas globales.

Figura 3.3.
Revolución digital y globalización en la configuración del ecosistema digital global.

Con la llegada de Trump a la presidencia de EE. UU. en 2017, se inicia una etapa de proteccionismo y geo-politización de las relaciones económicas (8) que se agudizará con la llegada de la pandemia y la guerra de Ucrania. Esta política se mantiene durante el mandato de Biden y se está llevando a extremos inimaginables en los primeros meses del segundo mandato de Trump.

En el nuevo contexto internacional, en el que se va sustituyendo el multilateralismo unipolar por un nuevo sistema multipolar, unos pocos polos van a gobernar el futuro digital del mundo. Europa quiere un lugar al lado de EE. UU. y China. De hecho, según Anu Bradford (9), en estos momentos compiten tres paradigmas: el propuesto por EE. UU. que defiende la primacía del mercado como fuente de innovación, prosperidad y libertad política; el propuesto por China que defiende la primacía del Estado como garante de la armonía social; y el propuesto por Europa que defiende la primacía de los valores, los derechos y el Estado de bienestar.

En consecuencia, el control de la producción y uso de las tecnologías digitales, y el dominio del ecosistema digital global se convierte en el elemento central de la nueva geopolítica ya que, como venimos señalando repetidamente, la transformación digital de la economía constituye la principal fuente de crecimiento económico y de la competitividad de las naciones. Además, los servicios digitales se prestan a nivel global y los datos de quienes los utilizan constituyen el nuevo activo clave en la economía digital. Una excelente descripción de este fenómeno puede verse en el apartado 1.4 de la fuente (10).

A mediados de la década de los noventa el desarrollo de las TIC hizo posible la denominada convergencia tecnológica, entendida como la capacidad de las infraestructuras de adquirir, almacenar, procesar, transportar y presentar simultáneamente voz, datos y vídeo. Ello abrió la posibilidad de desplegar nuevas aplicaciones y servicios que solapaban los mercados tradicionalmente separados de las telecomunicaciones, las TI (*hardware* y *software* informático) y el audiovisual.

La primera y definitiva gran convergencia fue Internet que permitió la integración de los datos, la voz, las imágenes y el video en los ordenadores personales y extender su conexión a todo el mundo, aprovechando, a pesar de sus limitaciones técnicas, la capilaridad de las redes telefónicas fijas tradicionales. El resultado fue la aparición de un espacio económico nuevo, la economía de Internet, que creció exponencialmente en las siguientes décadas generando nuevos agentes, algunos de los cuales han acabado convirtiéndose en las compañías de mayor valor bursátil del mundo.

En el año 2000, a pesar del pinchazo de la burbuja de las "empresas.com", la comunidad científico-técnica era consciente de que esta convergencia se aceleraría cuando se resolviese el "cuello de botella del acceso" (bucles de abonado fijos y móviles completamente digitales) y se popularice el acceso a Internet desde todo tipo de redes y terminales (teléfonos fijos, móviles, TV, etc.) además del acceso desde ordenador personal. Por otro lado, también era consciente de que esta convergencia de tecnologías acabaría convirtiéndose en una convergencia de mercados cuando la tecnología permitiese la integración efectiva de los servicios tradicionales de telefonía, datos y TV, y se superasen barreras que producían las distintas regulaciones sectoriales y su incapacidad para ordenar las infraestructuras y servicios de los mercados convergente. Una descripción completa de la situación descrita puede verse en la referencia: Grupo de Regulación de las Telecomunicaciones (GRETEL) (11).

En las dos décadas posteriores se produciría un desarrollo tecnológico impresionante que daría lugar a cuatro grandes innovaciones disruptivas sucesivas: la explosión de los dispositivos móviles, el auge de las redes sociales, la llegada de la nube y el surgimiento de la inteligencia artificial.

En los siguientes apartados vamos a describir el impacto de estas disrupciones tecnológicas en la creación del ecosistema digital.

3.3.1. La industria de las TIC se convierte en una industria global: especialización funcional y el protagonismo asiático

Durante el periodo comprendido entre los años 2000 y 2017, la industria de las Tecnologías de la Información y la Comunicación (TIC) experimentó una transformación sustantiva que la posicionó como un sector estratégico dentro de la economía mundial. Esta consolidación respondió tanto a procesos de innovación tecnológica como a dinámicas de integración económica internacional que favorecieron la formación de una cadena global de valor altamente especializada. En este contexto, diversas economías asumieron roles diferenciados en función de sus capacidades productivas, regulatorias y de innovación, generando un sistema interdependiente de producción, distribución y consumo de bienes y servicios digitales (12).

Un factor determinante en este proceso fue el papel desempeñado por la Organización

Mundial del Comercio (OMC), especialmente a través del Acuerdo sobre la Tecnología de la Información (ATI), suscrito inicialmente en 1996 y ampliado en 2015 (13). Este instrumento multilateral facilitó la eliminación de barreras arancelarias sobre una amplia gama de productos tecnológicos, promoviendo su libre circulación en los mercados internacionales. A ello se sumaron tratados de integración regional, tales como el Acuerdo Transpacífico (TPP) y el Tratado de Libre Comercio de América del Norte (TLCAN), los cuales consolidaron marcos normativos propicios para el intercambio de servicios digitales y para la movilidad de bienes tecnológicos, fortaleciendo la competitividad global del sector.

En este nuevo orden productivo, Asia desempeñó un papel particularmente destacado, configurándose como un centro de gravedad en la industria TIC tanto por su capacidad manufacturera como por sus avances en innovación tecnológica. China, en particular, emergió como un actor clave en la producción a gran escala de dispositivos electrónicos y componentes tecnológicos. Este posicionamiento fue el resultado de una estrategia estatal orientada a la modernización industrial, al fortalecimiento de capacidades locales en ingeniería y a la promoción de conglomerados tecnológicos con proyección internacional. Empresas como Huawei, Lenovo y ZTE constituyen ejemplos emblemáticos de este proceso, al haber transitado de tareas de ensamblaje hacia actividades de diseño, desarrollo e innovación.

Junto a China, otras economías asiáticas también adquirieron protagonismo. Corea del Sur destacó por su liderazgo en sectores intensivos en conocimiento, especialmente en el desarrollo de semiconductores, pantallas de alta resolución y redes de telecomunicaciones avanzadas. El compromiso sostenido con la investigación y el desarrollo (I+D), así como la cooperación estratégica entre el Estado y conglomerados empresariales —notablemente Samsung y LG—, permitió a Corea posicionarse como uno de los países tecnológicamente más avanzados del mundo. Japón, por su parte, mantuvo una posición de vanguardia en tecnologías de automatización, ingeniería de precisión y fabricación de componentes de alto valor agregado, consolidando su aporte en las etapas más complejas de la cadena de valor.

India se integró al sistema global de TIC desde una perspectiva distinta, especializándose en el desarrollo de *software* y la prestación de servicios digitales. La disponibilidad de capital humano altamente calificado y competitivo en términos salariales facilitó la expansión de sectores como la externalización de procesos de negocio (BPO), el desarrollo de aplicaciones y los servicios de soporte técnico. Esta especialización contribuyó a diversificar la estructura funcional de la industria y a fortalecer la complementariedad entre países productores de *hardware* y proveedores de soluciones digitales.

En el ámbito occidental, Estados Unidos conservó su hegemonía en la creación de plataformas digitales, generación de patentes tecnológicas y desarrollo de servicios digitales avanzados. Este liderazgo se sustentó en un entorno institucional favorable a la innovación y al emprendimiento, así como en una sólida infraestructura de investigación universitaria y empresarial. Europa Occidental, en cambio, orientó su contribución hacia la regulación del ecosistema digital, destacándose por la implementación de marcos normativos enfocados en la protección de datos, la competencia leal y los estándares de calidad y seguridad tecnológica. Su influencia normativa ha sido determinante en la configuración del comercio digital y en la gobernanza tecnológica a escala internacional.

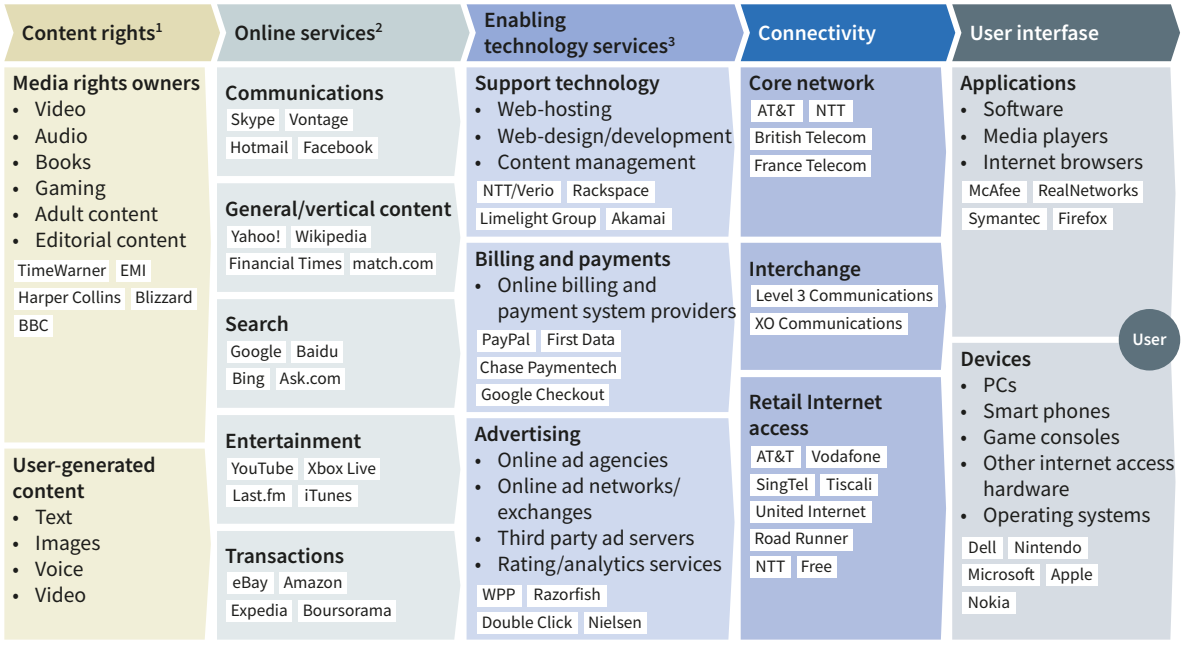
Asimismo, diversas economías emergentes, particularmente en América Latina y África, comenzaron a integrarse a este nuevo paradigma desde la demanda, con un crecimiento acelerado en el consumo de tecnologías digitales. Este proceso fue impulsado por el incremento del comercio electrónico, la masificación de dispositivos móviles y la expansión de la conectividad. Aunque estas regiones no desempeñaron roles protagónicos en la producción o innovación, representaron mercados en expansión que dinamizaron la demanda global de bienes y servicios tecnológicos.

En términos generales, la especialización geográfica funcional dentro del ecosistema TIC

generó una configuración global caracterizada por la interdependencia económica, la cooperación tecnológica y, a su vez, por nuevas tensiones asociadas a la competitividad, el empleo y la soberanía digital. El protagonismo de China y de otras economías asiáticas no se limitó únicamente a su capacidad productiva, sino que reflejó una reconfiguración más profunda del orden tecnológico mundial. Su ascenso como centros de innovación y manufactura ha contribuido a redefinir las jerarquías globales en el ámbito digital, constituyéndose en actores imprescindibles para comprender la evolución y los desafíos futuros de la economía digital global.

3.3.2. Internet una invención de Estados Unidos se extiende por todo el mundo

Entre los años 2000 y 2017, se produjo la adopción masiva de internet. En apenas una década y media, la conectividad digital dejó de ser un fenómeno restringido a ciertos grupos privilegiados para convertirse en una infraestructura esencial de la vida contemporánea. Durante este periodo, el número de usuarios de Internet creció de manera exponencial, al pasar de aproximadamente 413 millones en el año 2000 a más de 4.1 mil millones en 2017. Esta cifra representaba, para entonces, cerca del 54 % de la población mundial, constituyendo un punto de inflexión en la historia de la comunicación humana y el desarrollo tecnológico.



[1] Content rights abbreviated to CR in subsequent value chains
[2] See online services categories list in methodology for details
[3] Enabling technology/services abbreviated to ETS in subsequent value chains

Figura 3.4.
Cadena de valor de Internet en 2010.

Este vertiginoso crecimiento fue posible gracias a la convergencia de diversos factores, entre los que destaca el despliegue sostenido de infraestructuras de telecomunicaciones fijas y móviles. La expansión de redes móviles de tercera y cuarta generación (3G y 4G) permitió el acceso ubicuo a la red, particularmente en regiones donde las redes de cableado fijo eran limitadas o inexistentes. De igual manera, la proliferación de dispositivos móviles —en especial los

teléfonos inteligentes— jugó un rol determinante al facilitar la incorporación de amplios sectores sociales a los entornos digitales. En 2017, se contabilizaban más de 5 mil millones de usuarios de teléfonos móviles a nivel mundial, lo que consolidó estos dispositivos como la principal interfaz de acceso a Internet, y con ello, a una gama creciente de servicios y aplicaciones digitales.

Internet se convirtió, así, en el eje estructurante de un ecosistema digital en expansión, alrededor del cual se articularon nuevas formas de interacción social, producción económica y circulación de conocimiento. Las redes sociales constituyen uno de los fenómenos más paradigmáticos de esta transformación. Plataformas como Facebook —lanzada en 2004 y con más de 2 mil millones de usuarios activos para 2017— redefinieron las dinámicas de la comunicación interpersonal, la formación de identidades colectivas y la construcción de esferas públicas globales. A su lado, otras plataformas como X, Instagram y WhatsApp también alcanzaron una presencia masiva, consolidándose como medios esenciales para la diseminación de información y el intercambio instantáneo de mensajes, imágenes y videos. Estas plataformas, cuya existencia misma fue posibilitada por la infraestructura de Internet, no solo transformaron los hábitos comunicativos, sino que también introdujeron nuevas tensiones en torno al control de la información, la privacidad y la veracidad de los contenidos.

En el ámbito económico, Internet posibilitó el auge sin precedentes del comercio electrónico, alterando las lógicas tradicionales del mercado y la cadena de valor. Para 2017, las ventas globales en línea superaban los 2.3 billones de dólares, reflejando la consolidación de plataformas como Amazon, Alibaba y eBay como actores dominantes en la economía digital. El papel de Internet fue fundamental, no solo como canal de transacción comercial, sino también como espacio de innovación logística, gestión de datos, personalización del consumo y construcción de nuevos modelos de negocio. En particular, empresas asiáticas como Alibaba impulsaron el desarrollo de ecosistemas digitales integrales, en los cuales convergen comercio, medios de pago, publicidad y servicios en la nube. Este modelo, alimentado por el crecimiento exponencial del acceso a Internet en China y otras partes de Asia, demostró el potencial transformador de la conectividad digital en contextos económicos emergentes.

Para ilustrar este fenómeno en las **figura 3.4** (14) y **figura 3.5** (15) mostramos respectivamente la cadena de valor de Internet en el año 2010 y 2020.

El impacto de Internet también se manifestó con fuerza en el ámbito educativo y en la circulación del conocimiento. Iniciativas como Wikipedia democratizaron el acceso a información enciclopédica en múltiples idiomas y formatos, acumulando para 2017 más de 40 millones de artículos en casi 300 lenguas. A su vez, el desarrollo de plataformas de educación en línea como Coursera, edX y Khan Academy abrió nuevas posibilidades de formación académica, permitiendo el acceso a contenidos universitarios de alta calidad a millones de personas en contextos diversos. Estas plataformas, sustentadas completamente en tecnologías web, reconfiguraron las relaciones entre instituciones educativas, estudiantes y docentes, y pusieron en discusión los modelos tradicionales de enseñanza-aprendizaje. Países como India, China y Corea del Sur comenzaron a adoptar y adaptar estos modelos, generando sus propias plataformas nacionales y programas de alfabetización digital a gran escala.

Sin embargo, esta expansión global de Internet no estuvo exenta de desafíos y contradicciones. Uno de los más relevantes fue la persistencia de la brecha digital, entendida como la desigualdad en el acceso, uso y apropiación significativa de las tecnologías digitales. Mientras que en muchas economías desarrolladas las tasas de conectividad superaban el 80 %, regiones como África subsahariana apenas alcanzaban el 20 %. Estas disparidades no solo reflejan desigualdades económicas y geográficas, sino también limitaciones en términos de infraestructura, políticas públicas, alfabetización digital y disponibilidad de contenidos localmente relevantes. La brecha digital se convirtió, en este sentido, en un obstáculo estructural para la inclusión plena en el ecosistema digital global.

Paralelamente, la creciente centralidad de Internet en la vida cotidiana trajo consigo nuevas problemáticas asociadas a la privacidad de los datos personales, la ciberseguridad y la circulación de desinformación. La acumulación masiva de datos por parte de grandes plataformas tecnológicas, combinada con la falta de regulación efectiva en muchos países, generó un clima de creciente preocupación respecto a la protección de la intimidad digital y el uso comercial o político de la información personal. Asimismo, la velocidad con la que circulan contenidos en redes sociales dificultó la verificación de estos, facilitando la propagación de noticias falsas y discursos polarizadores, especialmente en contextos electorales o de crisis social.

En síntesis, el periodo 2000-2017 fue testigo de la consolidación de Internet como el núcleo articulador del ecosistema digital global. Su expansión masiva transformó radicalmente las

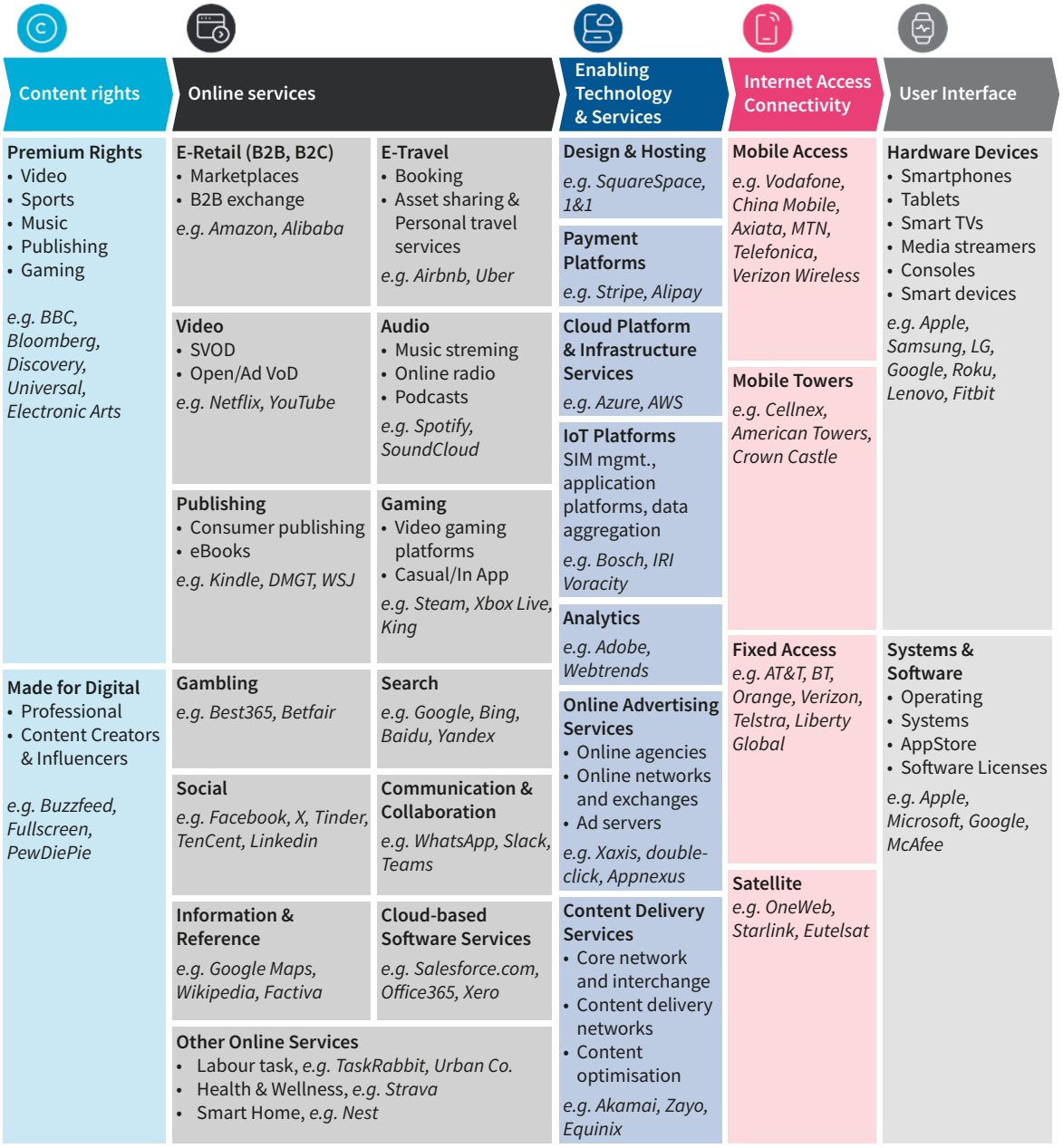


Figura 3.5.
Cadena de valor de Internet en el 2020.

formas de comunicarse, aprender, comerciar y participar en la vida pública, al tiempo que planteó nuevos dilemas en torno a la equidad, la gobernanza y los derechos digitales. Más que una mera herramienta tecnológica, Internet se constituyó como una infraestructura sociotécnica esencial que reconfiguró las estructuras mismas del mundo contemporáneo. Su papel central en la organización de las dinámicas digitales —desde lo económico hasta lo cultural— continuará siendo determinante para comprender las trayectorias futuras de la sociedad global.

3.3.3. El ecosistema digital es dominado por las plataformas de servicios de internet e *hiperscalers*

Entre los años 2000 y 2017, el panorama económico mundial experimentó una reconfiguración profunda, marcada por la emergencia de un nuevo tipo de actor económico: las plataformas digitales. Empresas como Google, Meta (anteriormente Facebook), Apple, Microsoft, Amazon, Tencent y Alibaba pasaron de ser firmas tecnológicas especializadas a convertirse en las compañías más valiosas del planeta por capitalización bursátil. Este ascenso no fue producto de un fenómeno aislado, sino de la convergencia de factores tecnológicos, económicos y sociales que favorecieron la centralización del poder económico, informacional y simbólico en torno a estas corporaciones.

La clave de este proceso radica en la transformación de estas empresas en infraestructuras digitales globales que estructuran y median gran parte de la actividad económica y social en línea. En sus inicios, estas compañías ofrecían productos o servicios específicos —un motor de búsqueda, una red social, un sistema operativo, una tienda en línea— pero con el tiempo evolucionaron hacia modelos de plataforma que organizan y controlan ecosistemas enteros de servicios, proveedores y usuarios. La rápida expansión de Internet, en paralelo con el despliegue de dispositivos conectados y la adopción global de servicios digitales, facilitó el acceso a estas plataformas, permitiendo a las empresas captar, procesar y monetizar cantidades sin precedentes de datos generados por individuos, organizaciones e instituciones públicas.

Un elemento distintivo del poder de estas empresas fue su capacidad para convertir los datos en un recurso económico central. Empresas como Google y Meta diseñaron modelos de negocio basados en la explotación de datos personales mediante sistemas de publicidad personalizada. A través del uso de algoritmos sofisticados, estas plataformas analizaron el comportamiento de los usuarios en tiempo real —sus búsquedas, clics, ubicaciones y preferencias— con el fin de ofrecer anuncios altamente segmentados, lo que multiplicó su rentabilidad. Este modelo de monetización les permitió generar ingresos masivos sin cobrar directamente por el acceso a sus servicios, lo que incentivó un crecimiento exponencial de su base de usuarios.

Paralelamente, otras compañías como Apple y Microsoft, inicialmente centradas en el desarrollo de *hardware* y *software*, se transformaron en plataformas integradas, ampliando su influencia más allá del dispositivo o sistema operativo. Apple, por ejemplo, articuló un ecosistema cerrado que vinculaba sus dispositivos con servicios digitales como iTunes, App Store, iCloud y Apple Pay, generando fidelización de sus usuarios e ingresos recurrentes. Microsoft, por su parte, combinó sus productos tradicionales como Windows y Office con la expansión de servicios en la nube y soluciones empresariales, consolidándose como una plataforma esencial para el mundo corporativo y educativo.

Un factor decisivo en este proceso fue el desarrollo y adopción de tecnologías habilitadoras como la computación en la nube, la inteligencia artificial (IA) y el análisis de Big Data. Estas tecnologías permitieron procesar grandes volúmenes de información de manera eficiente, lo que a su vez facilitó la innovación continua en productos y servicios. Plataformas como Amazon Web Services (AWS), Google

Cloud y Microsoft Azure se posicionaron como proveedores líderes de infraestructura digital, ofreciendo servicios esenciales a empresas de todos los sectores y tamaños. A través de estos servicios, las Big Tech no solo ofrecían productos finales, sino que también alquilaban capacidad computacional, almacenamiento y soluciones algorítmicas, consolidando su presencia en la columna vertebral del ecosistema digital.

En el contexto asiático, empresas como Alibaba y Tencent emergieron como referentes de un modelo de plataforma adaptado a los mercados emergentes, especialmente el chino. Su éxito se vio favorecido por un entorno regulatorio que limitó la competencia de grandes tecnológicas occidentales, permitiéndoles escalar rápidamente sus operaciones. Alibaba no solo lideró el comercio electrónico, sino que expandió sus actividades hacia la logística, la banca digital, la computación en la nube y los medios digitales. Tencent, por su parte, desarrolló plataformas integradas que combinaban mensajería, juegos, pagos móviles y servicios de contenido, con una capacidad de captación de usuarios que superó los mil millones. Ambas compañías demostraron cómo el modelo de plataforma podía adaptarse a contextos locales, al tiempo que reproducía dinámicas globales de concentración y expansión.

Uno de los mecanismos más importantes en la consolidación del poder de estas plataformas fue el efecto red, fenómeno por el cual el valor de una plataforma aumenta a medida que se suman más usuarios. A través de este mecanismo, las plataformas digitales lograron una expansión auto acelerada: cuantos más usuarios participaban en un servicio, más atractivo se volvía para otros usuarios, desarrolladores y anunciantes. Este efecto multiplicador consolidó posiciones dominantes en distintos segmentos del mercado digital, haciendo extremadamente difícil que nuevos competidores pudieran disputar ese poder. A ello se sumaron altas inversiones en investigación y desarrollo (I+D), lo que permitió a las grandes tecnológicas estar a la vanguardia de la innovación, anticipar tendencias tecnológicas y establecer estándares de facto.

Este conjunto de ventajas competitivas —acceso a datos masivos, economías de escala, control de infraestructuras críticas, fidelización de usuarios y capacidad de innovación— generó una barrera de entrada casi infranqueable para nuevas empresas. Como resultado, se produjo una concentración sin precedentes de valor y poder en torno a un pequeño grupo de corporaciones, cuyas valoraciones bursátiles crecieron de manera sostenida. La percepción positiva por parte de los inversores, alimentada por el potencial disruptivo de estas compañías, les permitió acceder a capital en condiciones muy favorables, lo cual a su vez facilitó adquisiciones estratégicas, como la compra de Instagram y WhatsApp por parte de Meta, o de LinkedIn por Microsoft. Estas operaciones no solo eliminaron competencia potencial, sino que ampliaron el alcance funcional y sectorial de las plataformas.

En última instancia, las plataformas digitales no solo transformaron el mercado tecnológico, sino que redefinieron los fundamentos de la economía global. Su capacidad para organizar mercados, influir en comportamientos, y mediar interacciones sociales y económicas las convirtió en actores clave no solo en términos comerciales, sino también políticos y culturales. El control sobre la infraestructura digital, los flujos de información y los patrones de consumo situó a estas empresas en una posición única desde la cual influir en políticas económicas, decisiones regulatorias y dinámicas de poder a nivel mundial.

3.4. GEOECONOMÍA DIGITAL

Existe un consenso creciente en torno a la imperiosa necesidad de avanzar hacia la digitalización de las economías. No obstante, los Estados enfrentan una serie de desafíos estructurales al momento de priorizar y asignar recursos escasos y presupuestos restringidos. Esta dificultad se intensifica al considerar que la transformación digital efectiva requiere un enfoque integral que abarque múltiples componentes interrelacionados: infraestructura

tecnológica robusta, capacidades humanas fortalecidas, marcos regulatorios adecuados y un entorno institucional dinámico que fomente la innovación.

Frente a este panorama, los formuladores de políticas públicas deben abordar una serie de interrogantes estratégicos. ¿Cuáles son las condiciones estructurales esenciales para habilitar una transformación digital sostenible? ¿Por qué ciertas economías logran utilizar las Tecnologías de la Información y la Comunicación (TIC) como catalizadores de desarrollo, mientras que otras permanecen rezagadas? ¿Cómo se puede armonizar la planificación estratégica centralizada con la innovación que emerge desde el ecosistema empresarial y social? ¿Qué rol deben asumir los sectores público y privado para garantizar una digitalización inclusiva y resiliente?

En este contexto, resulta evidente que no existe una fórmula única para lograr una digitalización exitosa. Cada nación requiere una hoja de ruta específica, adaptada a sus características estructurales, sus capacidades institucionales y sus prioridades de desarrollo. Esta personalización permite a los países no solo consumir tecnologías digitales, sino también participar activamente en su diseño, desarrollo y producción, insertándose en cadenas globales de valor de manera más productiva y autónoma.

Para facilitar este proceso, Arthur D. Little propone en su artículo *Think differently. Think archetype. Your digital economy model* un marco de referencia basado en arquetipos (16). Estos arquetipos no representan estados fijos ni modelos normativos, sino puntos de referencia estratégicos que orientan las decisiones nacionales de política digital en función de sus ventajas comparativas, capacidades existentes y aspiraciones de desarrollo.

El enfoque por arquetipos permite clasificar a las economías digitales en seis modelos fundamentales. Cada uno se caracteriza por una configuración particular de fortalezas, aspiraciones y desafíos, y conlleva estrategias diferenciadas en términos de inversión, gobernanza y colaboración público-privada. A continuación, se desarrollan estos arquetipos de forma más extensa, resaltando sus implicancias estratégicas, su aplicabilidad como guías para la acción política y ejemplos concretos de países que ilustran cada modelo, incluyendo los 27 Estados miembros de la Unión Europea. Un análisis detallado de la extracción de los arquetipos puede encontrarse en la fuente (17).

- **Núcleos de innovación** (*Innovation Hubs*). Este arquetipo agrupa a las economías más avanzadas tecnológicamente, que lideran la producción, comercialización y diseminación de tecnologías disruptivas. Estos países presentan una alta concentración de clústeres tecnológicos, universidades de élite, centros de I+D y un ecosistema emprendedor altamente dinámico. La innovación se encuentra en el núcleo de su modelo económico y se sustenta en fuertes capacidades científicas, una cultura empresarial propensa al riesgo y marcos regulatorios flexibles que permiten la experimentación.

  Ejemplos representativos incluyen a Estados Unidos, Corea del Sur e Israel. En la Unión Europea, este modelo es ejemplificado por Alemania, Suecia, Finlandia, Dinamarca, Irlanda y Países Bajos, países que destacan por su inversión en I+D, innovación empresarial y capacidad exportadora en sectores de alta tecnología.

- **Prosumidores avanzados** (*Efficient Prosumers*). Este modelo incluye a países que han logrado integrar tecnologías digitales en sectores estratégicos donde ya poseen ventajas competitivas. No necesariamente lideran la creación de nuevas tecnologías, pero destacan por su capacidad de adopción e integración eficiente.

  Alemania es un caso emblemático. En el contexto de la UE, también se incluyen Austria, Francia y los países nórdicos (Suecia, Finlandia, Dinamarca), donde las TIC se han integrado exitosamente en la educación, salud y administración pública, mejorando la productividad y el bienestar social.

- **Proveedores de servicios TIC** (*ICT Service Powerhouses*). Estos países se especializan en la provisión de servicios digitales a escala internacional, como *outsourcing* de

procesos empresariales (BPO), desarrollo de *software*, soporte técnico y análisis de datos. Cuentan con una población relativamente joven, una creciente base de educación técnica, dominio de lenguas extranjeras y costos operativos competitivos.

India y Filipinas son ejemplos globales destacados. En Europa, países como Polonia, Rumanía, Bulgaria y Hungría se posicionan dentro de este arquetipo, gracias a sus sectores de servicios digitales en expansión, el desarrollo de hubs tecnológicos regionales y políticas favorables a la inversión extranjera en TI.

- **Factorías tecnológicas** (*Global Factories*). Este arquetipo incluye a economías que basan su ventaja en la producción a gran escala de *hardware* y componentes tecnológicos. Estas naciones han desarrollado una infraestructura industrial sólida, acompañada de bajos costos laborales y una fuerte especialización en manufactura electrónica.

  China, México y Malasia lideran este modelo globalmente. En la Unión Europea, destacan República Checa, Eslovaquia y Eslovenia, países que han consolidado sectores manufactureros tecnológicamente avanzados, especialmente en componentes electrónicos y automoción digitalizada.

- **Nodos de negocios digitales** (*Digital Business Hubs*). Estos países funcionan como centros regionales para la gestión, comercialización y logística de bienes y servicios digitales. Se caracterizan por su conectividad, instituciones estables y una regulación favorable a la innovación.

  Singapur y Emiratos Árabes Unidos son referentes internacionales. En Europa, Países Bajos, Bélgica, Luxemburgo y Estonia actúan como nodos digitales estratégicos, albergando sedes regionales de empresas tecnológicas y plataformas de comercio electrónico, así como políticas gubernamentales que promueven la digitalización.

- **Consumidores sofisticados** (*ICT-Enabled Consumers*). Este arquetipo corresponde a economías con altos ingresos y elevados niveles de digitalización del consumo. Aunque no sean potencias productoras de tecnología, son mercados que adoptan rápidamente innovaciones y ofrecen oportunidades para la prueba y expansión de nuevos servicios digitales.

  Canadá y Australia se incluyen como ejemplos globales. Dentro de la UE, se pueden considerar en este grupo a España, Italia, Portugal, Grecia, Chipre, Malta, Croacia y Lituania, donde existe una alta penetración de internet y una ciudadanía digitalmente activa, aunque con menor capacidad productiva en el ámbito tecnológico.

Las naciones pueden aspirar a más, ya que es posible una movilidad limitada entre los arquetipos. Sin embargo, la transición llevará décadas y depende de las restricciones definidas por las dotaciones del país. Al participar o aumentar su presencia en actividades de TIC de mayor valor añadido, los países pueden aspirar a obtener mejores beneficios económicos y sociales y mejorar su posición o sus funciones en el ecosistema digital mundial. Por lo general, pasar a arquetipos de mayor valor añadido requiere un esfuerzo significativo tanto en términos de inversiones como de tiempo.

En la referencia mencionada, se describen diversos ejemplos de transiciones exitosas de arquetipos que han sido posibles gracias a medidas políticas deliberadas adoptadas por los gobiernos. Un caso destacado es el de Ucrania, que pasó de ser un actor incipiente en el ámbito de las tecnologías de la información y la comunicación (TIC) a convertirse en una potencia en servicios. En el año 2000, las exportaciones ucranianas de servicios de TIC alcanzaban apenas los 56 millones de dólares, situando al país en el puesto 52 a nivel mundial. Sin embargo, para 2017, Ucrania se había reposicionado como un centro relevante en servicios TIC, con exportaciones anuales que ascendían a 2.800 millones de dólares, ocupando así el puesto 25 a nivel global.

México también experimentó una evolución significativa, al pasar de ser un país incipiente en el sector de las TIC a convertirse en una plataforma de manufactura de alcance global. Similarmente, la República Eslovaca transitó de una posición de patrocinador de las TIC a la de

fábrica mundial en 2017. Sus exportaciones de bienes relacionados con las TIC pasaron de 0,4 mil millones de dólares en el año 2000 (puesto 41) a 13 mil millones de dólares en 2017 (puesto 19). La industria electrónica ha pasado a ser uno de los sectores económicos más relevantes del país, posicionándose como el segundo mayor empleador y exportador. Eslovaquia lidera a nivel regional en términos de productividad laboral, mientras mantiene una competitividad en costos tanto regional como europea. Esta transformación fue posible gracias a reformas en el entorno para hacer negocios y a inversiones estratégicas en el desarrollo de competencias de la fuerza laboral.

Por su parte, Rumania evolucionó de ser un patrocinador de las TIC a una potencia de servicios. En el año 2000, las exportaciones de servicios de TIC del país ascendían a 189 millones de dólares, ubicándose en el puesto 36 del *ranking* mundial. Para el año 2017, dichas exportaciones habían crecido hasta alcanzar los 4.500 millones de dólares, lo que situó a Rumania en la posición 21 a nivel mundial. Este avance puede atribuirse a la calidad de su sistema educativo en materia de TIC, tanto en el nivel secundario como universitario, a su competitiva relación calidad-precio, y a medidas adoptadas por el gobierno como la eliminación del impuesto sobre los salarios de los desarrolladores de software, la liberalización de precios, un régimen de comercio exterior abierto y el estímulo a la competencia leal en el sector de la información, lo que en conjunto fortaleció el clima de negocios y atrajo importantes inversiones.

Luxemburgo también representa un caso significativo, al haber pasado de ser un centro de negocios financieros a un prosumidor eficiente en su industria local dominante: los servicios financieros. Este cambio se logró mediante la implementación de políticas de agrupamiento que fortalecieron los vínculos entre empresas e instituciones de investigación, el fomento de un ecosistema de *start-ups* apoyado por fondos semilla como el Digital Tech Fund y el programa Fit4Start, la implementación de programas de habilidades digitales, *makerspaces*, escuelas tecnológicas, el programa Fit4Coding y centros de competencia en ciberseguridad, así como el desarrollo de estrategias específicas en fintech. Como resultado, las patentes en TIC se duplicaron entre 2000 y 2015, y el empleo en el sector TIC, en proporción al empleo total, se encuentra entre los más elevados de los países de la OCDE (18). En 2017, Luxemburgo ocupaba el octavo lugar en cuanto a patentes de TIC presentadas por millón de habitantes.

China, por otro lado, ha sido ampliamente reconocida por su transición de ser una fábrica global para convertirse en un núcleo de innovación. Actualmente, el país representa más del 20 % del gasto mundial en investigación y desarrollo. Esta transformación ha sido impulsada por inversiones continuas en investigación científica, el desarrollo de un plan nacional de inteligencia artificial, la creación de laboratorios nacionales de ingeniería y el establecimiento del mayor centro de investigación en computación cuántica a nivel global.

Finalmente, Finlandia ha protagonizado una evolución ejemplar, pasando de ser una economía enfocada en la manufactura de TIC en la década de 1990 —principalmente gracias al protagonismo de Nokia— a convertirse en una economía líder, orientada a la innovación en la actualidad.

Si la Unión Europea lograra consolidarse plenamente como un mercado único digital —mediante la implementación coordinada de políticas públicas, la integración de infraestructuras, la interoperabilidad transfronteriza y una estrategia común de innovación—, podría proyectarse como un núcleo de innovación de escala continental. Esta posibilidad se fundamenta en la existencia de múltiples condiciones estructurales favorables: una elevada inversión conjunta en I+D liderada por países como Alemania, Suecia, Finlandia y Países Bajos; un ecosistema científico-académico robusto; la presencia de empresas tecnológicas de referencia global; una ciudadanía digitalmente sofisticada; marcos regulatorios avanzados como el Reglamento General de Protección de Datos (RGPD) y la Ley de Servicios Digitales; y capacidades combinadas tanto en manufactura como en servicios TIC.

Asimismo, iniciativas como el programa Digital Europe (19), Horizon Europe (20) o la Brújula de competitividad refuerzan la viabilidad de esta proyección. No obstante, alcanzar dicha posición requeriría superar desigualdades internas en infraestructura digital, capacidades institucionales, niveles de inversión y competencias digitales entre los estados miembros. Solo mediante una implementación efectiva del mercado único digital, basada en la cohesión territorial y la interoperabilidad normativa y tecnológica, podría la Unión Europea constituirse plenamente como un actor líder en la economía digital global.

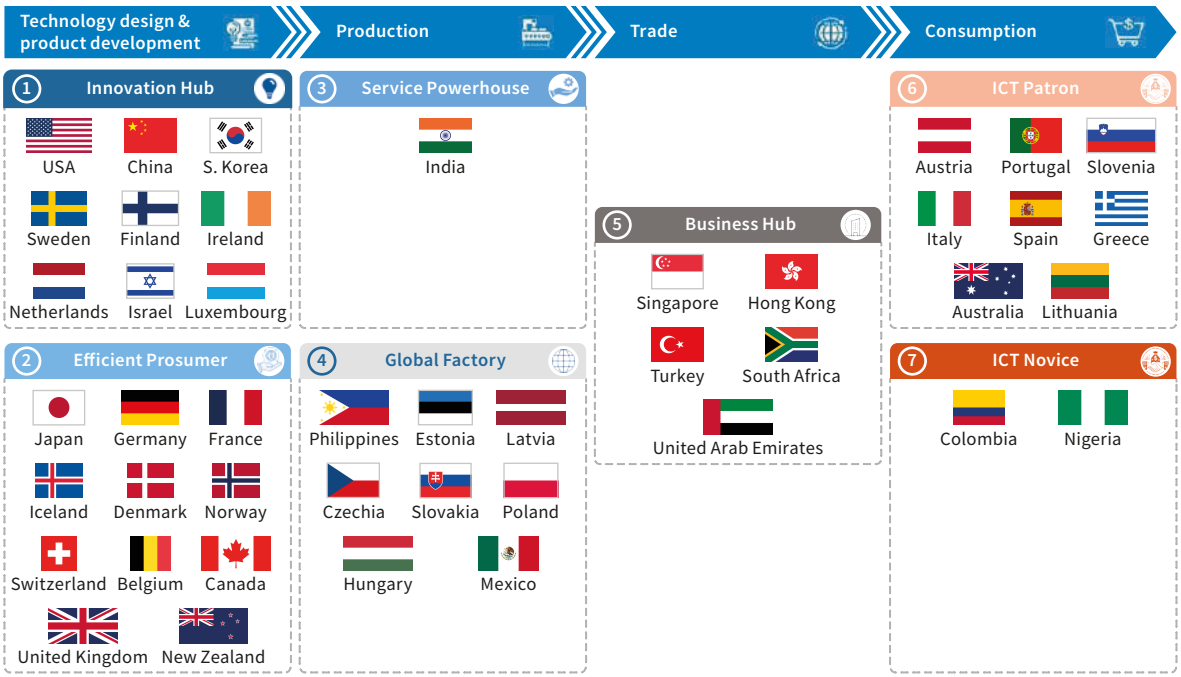


Figura 3.6.
Clasificación de países en arquetipos de economía digital.

3.5. DESAFÍOS PARA LA UNIÓN EUROPEA

La Unión Europea enfrenta una debilidad estructural en el ámbito económico frente a potencias como Estados Unidos y China, particularmente en el sector de las Tecnologías de la Información y la Comunicación (TIC). Mientras que Estados Unidos lidera la innovación tecnológica y la capitalización de las grandes empresas digitales, y China ha desarrollado una poderosa infraestructura tecnológica estatal, Europa se encuentra rezagada tanto en términos de inversión como de autonomía estratégica. Esta situación genera una dependencia tecnológica que compromete la competitividad y la soberanía digital del continente, haciendo urgente el desarrollo de estrategias coordinadas para fortalecer su ecosistema digital.

En este contexto, la UE está decidida a impulsar su competitividad tecnológica y capacidad de innovación mientras trabaja con socios y aliados para apoyar su propia transición digital. Se necesitan acuerdos internacionales con socios confiables que apoyen los intereses y valores fundamentales de la UE. Véase por ejemplo la estrategia propuesta recientemente por la alta representante de la unión para asuntos exteriores y política de seguridad: *Joint Communication to the European Parliament and the Council* (21).

La Estrategia Europea de Seguridad Económica (22) tiene como objetivo primordial fortalecer la resiliencia económica de la Unión Europea ante

riesgos tanto económicos como geopolíticos. Esta estrategia, presentada en junio de 2023, se articula en torno a tres ejes fundamentales: el fomento de la competitividad, la preservación de la seguridad económica y la cooperación internacional con socios fiables. La estrategia también reconoce una serie de riesgos clave, entre los que se encuentran la fragilidad de las cadenas de suministro, la ciberseguridad, las vulnerabilidades tecnológicas y la dependencia excesiva de países terceros.

En el marco de dicha estrategia, se han identificado un conjunto de tecnologías esenciales para salvaguardar la seguridad económica y estratégica de la Unión Europea. Estas tecnologías no solo buscan reducir la dependencia externa, sino también impulsar la autonomía estratégica europea y reforzar su competitividad global. Entre ellas destacan:

- Semiconductores. Elementos fundamentales para la industria tecnológica y la manufactura avanzada. La UE aspira a incrementar su capacidad productiva y minimizar su vulnerabilidad frente a proveedores extranjeros.
- Inteligencia Artificial (IA). Tecnología crucial para sectores como la salud, la agricultura, la industria y la ciberseguridad. La UE apuesta por un desarrollo regulado y ético que garantice su uso seguro.
- Tecnologías cuánticas. Comprenden la computación, sensórica y comunicaciones cuánticas, siendo claves para la protección de datos y la competitividad tecnológica.
- Energías limpias y tecnologías verdes. Constituyen una prioridad para alcanzar la descarbonización, asegurar la independencia energética y cumplir los compromisos climáticos.
- Ciberseguridad. Considerada esencial para la protección de infraestructuras críticas y datos estratégicos frente a amenazas externas.
- Biotecnología. Con aplicaciones en salud y agricultura, su desarrollo busca aumentar la resiliencia frente a crisis sanitarias y alimentarias.
- Tecnologías digitales avanzadas. Incluyen el despliegue de redes 5G y 6G, así como el fortalecimiento de competencias digitales en la ciudadanía.

Estas tecnologías cuentan con el respaldo de iniciativas como la Plataforma de Tecnologías Estratégicas para Europa (STEP) (23), que tiene como objetivo movilizar inversiones tanto públicas como privadas para su desarrollo y adopción generalizada.

En síntesis, el reto europeo consiste no solo en identificar las áreas críticas de intervención, sino también en articular de forma coherente sus políticas industriales, tecnológicas y de seguridad económica para cerrar la brecha que la separa de sus competidores globales. A continuación, analizaremos las políticas públicas europeas en las tecnologías digitales que no han sido analizadas en otros capítulos de este libro.

3.5.1. La inteligencia artificial como motor del futuro

La inteligencia artificial (IA) constituye uno de los vectores estratégicos más relevantes para la transformación digital, la soberanía tecnológica y la competitividad global de la Unión Europea. En el marco de la Brújula Digital para 2030, la UE se ha comprometido a alcanzar metas ambiciosas en conectividad, habilidades digitales, infraestructura de datos y digitalización de empresas y servicios públicos. En paralelo, la Brújula de la Competitividad, recientemente adoptada como instrumento complementario, refuerza el papel central de la innovación tecnológica —y especialmente de la IA— como motor de crecimiento económico sostenible, autonomía estratégica y bienestar social.

Dentro de este contexto, la IA se configura como una tecnología habilitadora transversal cuya implementación es crítica para alcanzar los objetivos establecidos por ambas brújulas. El desarrollo de una IA ética, confiable y centrada

en el ser humano no solo responde a imperativos normativos y de protección de derechos fundamentales, sino que también es una condición necesaria para consolidar un ecosistema europeo innovador, competitivo y resiliente frente a actores globales.

Para materializar esta visión, la Unión Europea ha desplegado una serie de políticas, marcos regulatorios e iniciativas estratégicas que conforman un enfoque integral hacia la inteligencia artificial. Desde la adopción del Reglamento de Inteligencia Artificial (2024) (24), orientado a establecer un entorno jurídico seguro y predecible para el desarrollo tecnológico, hasta el reciente paquete de medidas dirigidas a startups y pymes (25), la UE ha buscado simultáneamente garantizar la confianza ciudadana y promover la excelencia científica e industrial.

En esta misma línea, la Comisión Europea ha impulsado acciones específicas como las Directrices sobre prácticas de IA prohibidas (26), o la creación de la Academia de Habilidades en IA (27), que reflejan el compromiso de consolidar una base sólida para el despliegue amplio y responsable de estas tecnologías. Todas estas acciones no solo se alinean con los valores y principios europeos, sino que también refuerzan la capacidad de la UE para posicionarse como un actor global de referencia en inteligencia artificial.

Este entramado estratégico alcanza una nueva fase con el Plan de Acción del Continente de IA, que representa la iniciativa más ambiciosa hasta la fecha en el ámbito de la inteligencia artificial europea. A continuación, se analizan los pilares, objetivos y mecanismos de este plan, clave para afianzar el liderazgo digital de Europa en la era de la inteligencia artificial.

El Plan de Acción del Continente de IA, presentado por la Comisión Europea en su Comunicación (2025) 165 (28), constituye una estrategia ambiciosa y holística cuyo propósito es posicionar a Europa como un referente global en el desarrollo y aplicación de la inteligencia artificial (IA). Esta iniciativa surge en respuesta al creciente liderazgo tecnológico de potencias como Estados Unidos y China, así como a la necesidad urgente de reforzar la autonomía estratégica europea en tecnologías clave. El plan integra políticas industriales, científicas y sociales para movilizar recursos, coordinar actores y acelerar la adopción ética y sostenible de la IA en el continente.

Uno de los pilares fundamentales del plan es el establecimiento de al menos trece "factorías de IA" y hasta cinco "gigafactorías de IA" distribuidas en diferentes regiones europeas. Estas instalaciones se conciben como ecosistemas abiertos e interconectados que integran capacidades de supercomputación, grandes volúmenes de datos y talento humano especializado. Su objetivo es facilitar el desarrollo, entrenamiento y despliegue de modelos avanzados de IA, fomentando la colaboración entre empresas tecnológicas, centros de investigación, universidades y sectores industriales. Estas infraestructuras jugarán un papel estratégico en áreas de aplicación prioritarias como la salud, la transición ecológica, la manufactura avanzada y los servicios financieros.

El componente financiero del plan se articula en torno a la iniciativa "InvestAI", con la que se pretende movilizar hasta 200.000 millones de euros mediante la combinación de inversiones públicas y privadas. Esta movilización masiva de capital será instrumental para acelerar el desarrollo tecnológico y la escalabilidad de soluciones basadas en IA. El Banco Europeo de Inversiones desempeñará un rol clave como catalizador financiero, canalizando recursos hacia proyectos de alto impacto e impulsando la creación de valor en el ecosistema digital europeo.

En paralelo, el plan contempla la creación de un mercado único de datos, también denominado "Unión de Datos", destinado a facilitar el acceso a conjuntos de datos de alta calidad, interoperables y seguros. Este espacio común de datos es esencial para el entrenamiento eficaz de modelos de IA y para la democratización del acceso a recursos digitales fundamentales. Su diseño responde a la necesidad de superar la fragmentación actual del entorno europeo de datos, promoviendo una economía de datos inclusiva, competitiva y centrada en la ciudadanía.

La inteligencia artificial se desplegará de manera intensiva en sectores estratégicos seleccionados por su capacidad para generar externalidades positivas en el conjunto de la economía y la sociedad. Entre ellos se destacan la sanidad, el cambio climático, la fabricación inteligente y las finanzas. La aplicación transversal de tecnologías de IA en estos dominios busca maximizar su impacto estructural y contribuir a los objetivos de sostenibilidad, eficiencia y resiliencia del modelo socioeconómico europeo.

Asimismo, el plan incorpora un compromiso explícito con la sostenibilidad ambiental y la eficiencia energética. Las instalaciones tecnológicas impulsadas en este marco —incluidas las factorías y gigafactorías— estarán diseñadas para operar con neutralidad climática y para optimizar el consumo energético. Un ejemplo paradigmático de esta visión es el superordenador JUPITER, considerado uno de los más potentes y sostenibles del mundo, que representa un modelo de referencia para futuras infraestructuras digitales europeas.

Finalmente, la dimensión ética del plan es central y transversal. La Unión Europea reafirma su voluntad de liderar el desarrollo de una IA confiable, centrada en el ser humano y alineada con los valores democráticos y los derechos fundamentales. En este sentido, se prevé la implementación de marcos regulatorios que garanticen la transparencia, la seguridad y la rendición de cuentas en el uso de sistemas de IA, consolidando un enfoque europeo distintivo en la gobernanza tecnológica global.

En conjunto, el Plan de Acción del Continente de IA representa una apuesta estratégica por una inteligencia artificial que no solo sea tecnológicamente competitiva, sino también socialmente responsable, sostenible y alineada con los principios fundacionales del proyecto europeo.

3.5.2. La computación cuántica

En el contexto de la Estrategia para la Década Digital de la Unión Europea, que define las prioridades para asegurar una transición digital justa, inclusiva y soberana, la Declaración Europea sobre Tecnologías Cuánticas (29), firmada inicialmente en diciembre de 2023, se erige como un hito fundamental. Esta declaración constituye un compromiso político y estratégico de los Estados miembros para liderar el desarrollo de un ecosistema cuántico de clase mundial. En ella se reconocen las tecnologías cuánticas no solo como un vector de innovación científica, sino también como un instrumento esencial para la soberanía tecnológica, la seguridad de las infraestructuras críticas y la competitividad industrial de Europa en el escenario global. Su implementación está estrechamente vinculada a otros marcos clave, como la Ley Europea de Chips, que persigue reforzar las capacidades de diseño y producción de semiconductores avanzados, y al despliegue del primer superordenador europeo con aceleración cuántica, previsto dentro del marco de la Empresa Común EuroHPC (30).

La declaración plantea como objetivo central convertir a Europa en el "valle cuántico" del mundo, equiparando su papel en este ámbito al de Silicon Valley en las tecnologías digitales. Este propósito implica construir un ecosistema profundamente integrado, en el que confluyan la investigación básica, el desarrollo tecnológico, la innovación aplicada y la industrialización de soluciones cuánticas. Las áreas prioritarias de trabajo comprenden la computación cuántica —con la ambición de resolver problemas de alta complejidad en sectores como la salud, la logística o la inteligencia artificial—, las comunicaciones cuánticas —particularmente mediante el desarrollo de la Infraestructura Europea de Comunicación Cuántica (EuroQCI), que garantizará una transmisión de datos segura ante amenazas cuánticas—, y la sensórica cuántica, con aplicaciones estratégicas en medicina de precisión, protección ambiental y sistemas de defensa.

La adhesión de veintiséis estados miembros, entre ellos Alemania, Francia, España e Italia, a

esta declaración refleja el compromiso colectivo de avanzar en la coordinación de políticas públicas, investigación transfronteriza y despliegue conjunto de infraestructuras. Este impulso se sustenta en instrumentos financieros del Marco Financiero Plurianual de la UE, como el programa Horizonte Europa, así como en asociaciones estratégicas como EuroHPC, que promueve el desarrollo de capacidades europeas en supercomputación de alto rendimiento. Además, iniciativas emblemáticas como el Buque Insignia Cuántico, lanzado en 2018 con una dotación de mil millones de euros a diez años, proporcionan un marco estructurado para la financiación de proyectos de investigación e innovación en tecnologías cuánticas.

El impacto esperado de esta apuesta tecnológica es múltiple. Se anticipa una transformación sustancial de industrias clave mediante la aplicación de soluciones cuánticas, al tiempo que se fortalece la autonomía estratégica europea en un contexto geopolítico caracterizado por la competencia tecnológica global. Asimismo, se prevé un salto cualitativo en la producción de conocimiento científico, posicionando a Europa como un referente mundial en física cuántica y en el desarrollo de sus aplicaciones. En definitiva, la Declaración Europea sobre Tecnologías Cuánticas representa una piedra angular en la configuración de una Europa digitalmente soberana, innovadora y resiliente, plenamente alineada con los objetivos estructurales de la década digital y con una visión estratégica a largo plazo para el liderazgo en la computación cuántica global.

En este contexto de impulso paneuropeo a las tecnologías cuánticas, emergen iniciativas nacionales que buscan consolidar la contribución de los estados miembros a este esfuerzo colectivo. Un caso paradigmático es el de España, cuya apuesta por la computación cuántica se ha materializado en la iniciativa Quantum Spain (31), un proyecto emblemático orientado a integrar esta tecnología en el ecosistema científico, tecnológico e industrial del país. Liderado por el Barcelona Supercomputing Center (BSC-CNS) y articulado en torno a una red de 27 instituciones de excelencia, Quantum Spain tiene como objetivos fundamentales la creación de un entorno colaborativo para el desarrollo cuántico, el impulso de soluciones de inteligencia artificial mediante computación cuántica, y el fortalecimiento de la soberanía tecnológica nacional.

La infraestructura del proyecto se apoya en los 14 nodos de la Red Española de Supercomputación (RES), incluyendo entidades como el CSIC, el ICFO y diversas universidades de referencia. Su financiación proviene del Plan de Recuperación, Transformación y Resiliencia, en el marco de la agenda España Digital 2026 y la Estrategia Nacional de Inteligencia Artificial (ENIA), lo que refuerza su alineación con las prioridades estratégicas del país y de la Unión Europea.

Uno de los hitos más relevantes del proyecto es la integración de un ordenador cuántico con tecnología 100 % europea en el supercomputador MareNostrum 5, situado en el BSC. Esta combinación de computación clásica y cuántica permitirá abordar problemas de elevada complejidad en ámbitos como la simulación de materiales, la optimización logística y la ciberseguridad, posicionando a España como un nodo estratégico en el futuro cuántico de Europa.

Quantum Spain constituye, por tanto, un ejemplo destacado de cómo la colaboración entre instituciones públicas y privadas puede traducirse en avances significativos para la innovación tecnológica, la generación de conocimiento y la mejora de la competitividad industrial. Su impacto se proyecta no solo en términos de desarrollo científico, sino también en la creación de empleo altamente cualificado y en el refuerzo de la autonomía digital europea. Su evolución y resultados serán, sin duda, un elemento clave a seguir dentro del panorama cuántico europeo.

Un informe reciente del Real Instituto Elcano ha realizado el análisis de las tecnologías cuánticas como una oportunidad estratégica para Europa y España en el contexto de competencia global con EE. UU. y China (32).

3.5.3. Semiconductores (33)

En un contexto de crecientes tensiones geopolíticas, disrupciones en las cadenas de suministro globales y una acelerada transformación digital, la Unión Europea ha identificado los semiconductores como un componente esencial para salvaguardar su autonomía estratégica y consolidar su liderazgo en el ecosistema digital. La iniciativa conocida como la Ley Europea de Chips (*European Chips Act*) (34) representa un paso decisivo hacia la reindustrialización tecnológica del continente, con el objetivo de garantizar una capacidad de producción sólida, resiliente y competitiva en el ámbito de los semiconductores.

Los semiconductores son fundamentales para una amplia gama de sectores estratégicos, incluyendo la salud, el transporte, la energía, la inteligencia artificial y la defensa. En este sentido, la Ley de Chips busca no solo duplicar la cuota de producción mundial de la UE en este ámbito hasta alcanzar el 20 % para 2030, sino también establecer un entorno propicio para la innovación, la atracción de inversiones y la formación de talento especializado. La estrategia pretende crear un ecosistema integral que permita a Europa reducir su dependencia de proveedores externos, responder con mayor agilidad a crisis de suministro y posicionarse como un actor clave en el mercado global de tecnologías avanzadas.

La Recomendación (UE) 2022/210, adoptada por la Comisión Europea el 8 de febrero de 2022, aborda la escasez de semiconductores y propone medidas para fortalecer la resiliencia de la cadena de suministro en Europa. Esta iniciativa surge como respuesta a las interrupciones sin precedentes que afectaron a sectores críticos como la salud, el transporte, la energía y la defensa. Su objetivo principal es establecer un conjunto de herramientas comunes y un mecanismo de coordinación eficaz entre los estados miembros y la Comisión para responder de manera ágil a las crisis relacionadas con el suministro de semiconductores. Entre las medidas clave se encuentra la creación de un sistema de coordinación para debatir y decidir acciones oportunas, así como el establecimiento de un sistema de monitoreo coordinado que permita identificar riesgos en la cadena de valor. Asimismo, se busca fomentar el desarrollo de capacidades de fabricación, diseño e integración avanzada en el ámbito de los semiconductores, y abordar la escasez de profesionales cualificados mediante programas de formación. El impacto esperado de estas medidas se traduce en una mayor resiliencia frente a interrupciones en el suministro, un fortalecimiento de la competitividad europea en el contexto de la transición digital y ecológica, y el avance hacia una soberanía tecnológica que permita a la UE alcanzar el objetivo estratégico de producir al menos el 20 % del valor mundial de semiconductores avanzados para el año 2030.

3.6. CONCLUSIONES

- En las dos últimas décadas el ecosistema digital ha dejado de ser un sector marginal asociado exclusivamente a las tecnologías de la información y la comunicación para convertirse en una arquitectura económica transversal que redefine las dinámicas productivas y competitivas a escala global. Esta transformación se manifiesta en la creciente participación de las empresas digitales en los beneficios económicos mundiales, su capacidad para atraer inversión en innovación y su rol como catalizador de nuevas industrias y modelos de negocio. A través de la interconexión de infraestructuras, plataformas y servicios, el ecosistema digital ha consolidado su posición como un pilar estructural de la economía del siglo XXI.
- Si bien el ecosistema digital se caracteriza por su apertura a la innovación y la entrada de nuevos competidores, este dinamismo convive con una marcada concentración del mercado en manos de un número

reducido de grandes corporaciones tecnológicas. Esta dualidad evidencia tanto el potencial democratizador de las tecnologías digitales como los riesgos asociados a la acumulación de poder económico y de datos. La capacidad de estas empresas para escalar globalmente y establecer efectos de red plantea desafíos significativos para la competencia y la regulación, especialmente en contextos donde las fronteras geográficas y normativas tradicionales se diluyen frente a la expansión digital.

- El periodo 2000-2017 estuvo marcado por una profunda interconexión entre revolución tecnológica y globalización económica, que dio lugar a una cadena de valor digital altamente segmentada. Bajo la dinámica de libre comercio y la garantía de seguridad proporcionada por Estados Unidos, cada región se especializó en eslabones específicos de la producción digital —desde fabricación masiva de *hardware* en Asia hasta desarrollo de *software* y servicios en India y Occidente—, consolidando un ecosistema digital interdependiente cuya eficiencia y resiliencia se sustentaron en la cooperación transfronteriza.
- La confianza geopolítica vivida entre el 2000 al 2017 facilitó el despliegue masivo de Internet y tecnologías convergentes (móvil, social, nube, IA), pero el viraje hacia políticas proteccionistas y la emergencia de paradigmas tecno-nacionalistas a partir de 2017 evidenciaron la fragilidad de ese consenso. La transición hacia un orden multipolar, con EE. UU., China y la Unión Europea compitiendo por modelos contrastados de gobernanza digital, pone de manifiesto la tensión entre innovación, concentración de poder en grandes plataformas y la necesidad de soberanía tecnológica y regulatoria.
- El análisis demuestra que la digitalización efectiva no puede basarse en un modelo uniforme, sino que exige marcos de política adaptados a las condiciones estructurales y al grado de desarrollo institucional de cada Estado. El uso de arquetipos —desde núcleos de innovación hasta consumidores sofisticados— permite identificar rutas de progreso diferenciadas y focalizar recursos en fortalezas comparativas, favoreciendo trayectorias de transformación más coherentes y sostenibles.
- A pesar del potencial económico y tecnológico de la Unión Europea, persisten brechas internas y dependencia de proveedores externos en áreas críticas como semiconductores, inteligencia artificial y computación cuántica. Solo una estrategia coordinada a nivel comunitario —que articule políticas industriales, marcos regulatorios, financiación y desarrollo de capacidades— podrá cerrar estas brechas y posicionar al bloque como un mercado digital verdaderamente integrado y autónomo.

3.7. REFERENCIAS BIBLIOGRÁFICAS

1. OECD. Measuring the Information Economy 2002 [Internet]. Paris: OECD Publishing; 2002. DOI: https://doi.org/10.1787/9789264099012-en
2. Tapscott D. The digital economy: promise and peril in the age of networked intelligence. New York: McGraw-Hill; 1997. ISBN 0-07-063342-8.
3. Bukht R, Heeks R. Defining, Conceptualising and Measuring the Digital Economy. International Organisations Research Journal. 2018; (13):143-172. DOI:10.17323/1996-7845-2018-02-07
4. International Monetary Fund. Measuring the Digital Economy [Internet]. 2018 [citado 16 de abril de 2025]. Disponible en: https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy

5. Pérez J, Rodríguez P. La Gobernanza y regulación del ecosistema digital. La visión de la Unión Europea. En: González É, Herrera LM, Murguitio J, Ortiz SM. Las TIC y la sociedad digital: doce años después de la ley. Tomo II, el ecosistema digital en sus distintos desarrollos y las tecnologías disruptivas. Bogotá: Universidad Externado de Colombia; 2021. p. 263-299.

6. Renda A. Conference given in ETSIT of the Universidad Politécnica 21-11-2019.

7. Bradley C, Chui M, Russell K, Ellingrud K, Birshan M, Chettih S. The next big arenas of competition [Internet] McKinsey Global Institute; 2023 [citado 20 de abril de 2025]. Disponible en: https://www.mckinsey.com/mgi/our-research/the-next-big-arenas-of-competition

8. Mearsheimer J. Bound to Fail: The Rise and Fall of the Liberal International Order. International Security. 2019; vol. 43, nº4. p. 7-50.

9. Bradford A. Imperios digitales. La batalla global por la tecnología que marcará la geopolítica del futuro. Shackleton Books; 2024. ISBN: 9788413615028.

10. Pérez J, Hernández-Gil JF, Arteaga F, Martín JL. El futuro digital de Europa [Internet]. Madrid: Taurus; 2020. ISBN: 9788430699414. Disponible en: https://www.fundaciontelefonica.com/cultura-digital/publicaciones/el-futuro-digital-de-europa/714/

11. GRETEL 2000: Convergencia, competencia y regulación en los mercados de Telecomunicaciones, el audiovisual e internet [Internet]. Editorial COIT; 2020. Disponible en: https://forohistorico.coit.es/index.php/biblioteca/libros-electronicos/item/gretel-2000-convergencia-competencia-y-regulacion-en-los-mercados-de-telecomunicaciones-el-audiovisual-e-internet

12. OECD. OECD Digital Economy Outlook 2017 [Internet]. OECD Publishing; 2017. Disponible en: https://doi.org/10.1787/9789264276284-en

13. World Trade Organization. Acuerdo sobre Tecnología de la Información. Informe Anual 2016 [Internet]. WTO Library; 2016 may 23. [citado 24 de abril de 2025]. Disponible en: https://doi.org/10.30875/b59af4d5-es

14. Kearney A. Internet Value Chain Economics [Internet]. A.T. Kearney, Inc.; 2010 [citado 20 de abril de 2025]. Disponible en: https://www.kearney.com/documents/291362523/291364109/internet-value-chain-economics.pdf/285d1a4d-a49c-43d1-5966-9fcca69aa55a?t=1493922220000

15. Freyberg A, Rand C. The Internet Value Chain [Internet]. GSMA; 2022 [citado 20 de abril de 2025]. Disponible en: https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2022/05/Internet-Value-Chain-2022-1.pdf

16. Baes K, Chen J, Cheng Q, Duneja R, Prakash Iyer S, Kanakamedala V, Yang J. Think differently. Think archetype. Your digital economy model [Internet]. Arthur D. Little, Huawei; 2020 [citado 24 de abril de 2025]. Disponible en: https://www-file.huawei.com/-/media/corp2020/pdf/public-policy/adl_huawei_digital_transformation_main_report.pdf?la=en-us

17. Rodríguez P. East Wind, West Wind. Analysis of the European Digital Ecosystem in the context of a technological cold war. ETSIT UPM; 2023.

18. OECD Going Digital Toolkit 2025 [Internet]. OECD Going Digital Toolkit. Disponible en: https://goingdigital.oecd.org/

19. Unión Europea. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 [Internet]. Europa.eu; 2021 [citado 24 de abril de 2025]. Disponible en: http://data.europa.eu/eli/reg/2021/694/oj

20. Unión Europea. Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 [Internet]. Europa.eu; 2021 [citado 24 de abril de 2025]. Disponible en: http://data.europa.eu/eli/reg/2021/695/oj

21. Unión Europea. Joint Communication to the European Parliament and the Council. An International Digital Strategy for the European Union [Internet]. JOIN(2025) 140 final; 2025 [citado 24 de abril de 2025]. Disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:e346392e-41ed-11f0-b9f2-01aa75ed71a1.0001.02/DOC_1&format=PDF

22. Comisión Europea (Dirección General de Comunicación). Estrategia europea de seguridad económica [Internet]. Oficina de Publicaciones de la Unión Europea; 2023. Disponible en: https://data.europa.eu/doi/10.2775/236251

23. Consejo de la Unión Europea. Proposal for a Regulation of the European Parliament and of the Council Establishing the Strategic Technologies for Europe Platform ('STEP') [Internet]. Councill of the European Union; 2024 [citado 24 de abril de 2025]. Disponible en: https://data.consilium.europa.eu/doc/document/ST-5241-2024-REV-1/en/pdf

24. Unión Europea. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [Internet]. Europa.eu; 2024. Disponible en: http://data.europa.eu/eli/reg/2024/1689/oj

25. Comisión Europea. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions SME Relief Package [Internet]. Europa.eu; 2023. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0535

26. Comisión Europea. Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) [Internet]. Europa.eu; 2025. Disponible en: https://digital-strategy.ec.europa.eu/es/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

27. Comisión Europea. EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence [Internet]. Press Release; 2025. Disponible en: https://digital-strategy.ec.europa.eu/en/news/eu-launches-investai-initiative-mobilise-eu200-billion-investment-artificial-intelligence

28. Comisión Europea. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions AI Continent Action Plan [Internet]. Europa.eu; 2025. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0165

29. Comisión Europea. Declaración Europea sobre Tecnologías Cuánticas [Internet]. Europa.eu; 2023. Disponible en: https://digital-strategy.ec.europa.eu/es/library/european-declaration-quantum-technologies

30. Unión Europea. Council Regulation (EU) 2024/1732 of 17 June 2024 amending Regulation (EU) 2021/1173 as regards a EuroHPC initiative for start-ups in order to boost European leadership in trustworthy artificial intelligence [Internet]. Europa.eu; 2024. Disponible en: http://data.europa.eu/eli/reg/2024/1732/oj

31. Quantum Spain | España Digital 2026 [Internet]. Espanadigital.gob.es; 2024. Disponible en: https://espanadigital.gob.es/lineas-de-actuacion/quantum-spain

32. Arizaga Í, Gil G, Ayerbe A, Arnal J, Ricart R. Tecnologías cuánticas cómo apostar y acertar desde España y la UE [Internet]. Real Instituto Elcano; 2025. Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2025/04/policy-paper-tecnologias-cuanticas-como-apostar-y-acertar-desde-espana-y-la-ue.pdf

33. García EG, Jiménez M. Chips y poder. Una batalla global por controlar la tecnología del futuro. Catarata; 2025. ISNN: 9788410672604.

34. Unión Europea. Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) [Internet]. Europa.eu; 2023. Disponible en: http://data.europa.eu/eli/reg/2023/1781/oj

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

4

Geopolítica digital. La autonomía digital estratégica de la UE

Emilio García García

4.1. LA QUEBRANTADA AUTONOMÍA DIGITAL ESTRATÉGICA DE EUROPA

La autonomía estratégica no es un concepto nuevo en el léxico político de la Unión Europea, sino que nace en 2016 en el ámbito de la defensa y seguridad. La referencia base del concepto son las Conclusiones del Consejo de 2016, donde se define como la "capacidad para actuar de manera autónoma cuando y donde sea necesario y, en la medida de lo posible, con los países asociados" (1). El concepto ha sido extendido después a distintos ámbitos sectoriales, en el caso de la autonomía estratégica en el ámbito digital, desde Europa siempre se ha observado la misma en relación con Estados Unidos. Con la extensión de la tecnología a toda área de actividad, preservar la autonomía digital estratégica ha pasado a ser un pilar clave en la seguridad económica.

El gigante del nuevo continente se ha identificado como el país asociado con el que la Unión Europea actúa conjuntamente en el entorno digital global. La alianza no ha estado exenta de tensiones por las distintas visiones que ambas áreas económicas han mantenido históricamente del desarrollo tecnológico. Desde Estados Unidos, se ha promovido una digitalización dirigida fundamentalmente por las fuerzas del mercado, considerando la intervención pública en esta esfera una traba al impulso innovador del sector privado. Desde Europa, la intervención regulatoria se ha impulsado como un elemento imprescindible de las políticas públicas digitales, como garantía de la traslación de los derechos y valores existentes en el mundo físico a la esfera digital.

En la primera década del siglo XXI, cuando la ola de innovación impulsada por Internet se comenzó a conformar como el tsunami de la digitalización, las visiones del desarrollo tecnológico mantenidas por la UE y EE. UU. eran vistas como complementarias. En el mundo multilateral surgido de la Guerra Fría se veía la pugna entre ambas áreas económicas como relativamente amistosa y garantía de una transformación digital global equilibrada. Tampoco se concebía en la esfera internacional la autonomía digital como un valor a construir y preservar, sino como algo inherente a la globalización. En un mundo basado en el libre comercio, las cadenas de suministro globales eran la garantía de un acceso abierto a los bienes y servicios tecnológicos, y las alianzas tenían una geometría variable sin temor a la generación de dependencias tóxicas.

La progresiva emergencia de China como potencia mundial astilló el modelo de desarrollo multilateral abierto, y en particular en la esfera digital. El gigante asiático quiso traducir su poder económico en desarrollo tecnológico soberano, con una concepción de la digitalización basada en la primacía del Estado (y sus objetivos) sobre el mercado y las personas. Esta visión de la digitalización del gigante asiático rivalizaba a la vez con los modelos europeos y estadounidense, desafío frente al que las élites políticas de ambos bloques impulsaron una colaboración en la esfera tecnológica a partir de la década de 2010, aunque no exenta de aristas y altibajos. La cooperación trasatlántica era vista desde las dos orillas como una garantía mutua de su autonomía digital, frente a un ecosistema chino que buscaba una autosuficiencia que, además, era utilizada como palanca para aspirar al dominio mundial sustentado sobre la estrategia de circulación dual (2).

No puede extraer Europa una conclusión positiva de su papel de escudero de los intereses de Estados Unidos en la esfera digital. La UE ha visto impotente cómo en los últimos quince años las empresas del continente que fueron dominantes en el ecosistema digital han desaparecido —caso de la sección de gran consumo de Nokia— o disminuido drásticamente su capitalización bursátil —coyuntura de las operadoras de telecomunicaciones—, sin que haya surgido una generación de firmas tecnológicas de relevo. De modo especular, en esta última década se ha producido un crecimiento, por momentos exponencial, del tamaño de las empresas tecnológicas estadounidenses. Tras la irresistible escalada bursátil que inició Nvidia en 2022, a finales de 2024 ocho de las diez mayores firmas por capitalización

son compañías estadounidenses de base tecnológica. Mientras, las dos primeras empresas del sector digital localizadas en Europa estaban por debajo de las treinta de mayor tamaño.

La jibarización digital de Europa ha sido pareja a su pérdida de peso en la economía global, demostrando de modo inequívoco la relación de este con la autonomía digital estratégica. De acuerdo con un informe publicado por la empresa McKinsey, en los últimos diez años el PIB de Estados Unidos ha crecido de alrededor de los 16 trillones (trillón americano) de dólares hasta 26 trillones de dólares (3). El ritmo de crecimiento de la economía estadounidense le ha permitido superar el PIB europeo, habiendo pasado entre 2013 y 2023 de una inferioridad porcentual de 14 puntos porcentuales a una superioridad de 17 puntos.

A pesar que la senda de declive tecnológico del viejo continente fue paulatinamente manifiesta en esta configuración de alianzas, la colaboración en la esfera digital con Estados Unidos y Europa se hizo aún más estrecha en los últimos cuatro años. En los foros internacionales, como el G20 o la Unión Internacional de Telecomunicaciones, las posiciones de las dos áreas económicas fueron cada vez menos complementarias y más convergentes. También cogió forma la institucionalización de esta alianza. Tras diversos intentos infructuosos, emergió tras la pandemia de la COVID-19 el Consejo de Comercio y Tecnología (CCT) como instrumento de articulación de una asociación estable. El consejo fue establecido en junio de 2021 como uno de los resultados de la cumbre entre la UE y EE. UU. y definió como objetivos cooperar en políticas clave sobre tecnología, cuestiones digitales y cadenas de suministro.

El foco de la colaboración digital de la UE y EE. UU. en el CCT estuvo en las áreas de semiconductores, inteligencia artificial y tecnologías cuánticas. No es casual este hecho. La Comisión Europea, ha señalado tres tecnologías críticas como centrales para su seguridad tecnológica y económica futura (4). También Mario Draghi, selecciona estas áreas del sector digital, junto con las telecomunicaciones, como pilares de la competitividad futura de Europa (5) (6).

La colaboración de la UE con EE. UU. no ha supuesto una mejora relevante de las capacidades tecnológicas europeas. De acuerdo con el *benchmarking* realizado anualmente del Instituto de Políticas Estratégicas de Australia —evaluación del rendimiento de la investigación, intención estratégica y potencial capacidad científica y tecnológica futura en 70 tecnologías críticas— China y EE. UU. lideran el desarrollo de diseño avanzado de circuitos integrados, computación cuántica y procesamiento de lenguaje natural, claves en las tres tecnologías críticas digitales del futuro (7), acumulando casi un 50 % de las capacidades mundiales de modo conjunto en todas ellas y marcando cada vez más distancia con Europa.

La situación no es mejor en la cuarta pata que ha de sustentar la mesa de la autonomía digital estratégica de la UE: las telecomunicaciones. La Comisión Europea estimó en más de 200.000 millones de euros las inversiones necesarias para habilitar despliegue de redes de fibra y 5G que respondan a los objetivos de la Década Digital, en 2025, según la evaluación de Analysys Mason, aún tendrían que materializarse hasta 2030 inversiones por valor de 100.000 millones (8). La UE inició una consulta pública en 2023 a la búsqueda de un escenario que garantice la disponibilidad futura de redes de telecomunicaciones acordes con estas necesidades. La alternativa prioritaria barajada por la Comisión para desencadenar esa inversión era la imposición de una contribución justa (*fair share*) a las grandes tecnológicas estadounidenses para facilitar el desarrollo de las redes de telecomunicaciones europeas, de las que son usuarias intensivas. La falta de unanimidad entre los estados miembros hizo embarrancar la idea sin existir una propuesta de recambio.

En definitiva, Europa ha continuado diluyendo durante la legislatura 2019-2024 una parte sustancial de su soberanía digital en EE. UU., ligando a la alianza trasatlántica su desarrollo digital y, con ello, su seguridad económica. Un bagaje de resultados que resulta paradójico para una Comisión Europea que su presidenta presentó como “Geopolítica” en su discurso de investidura en septiembre de 2019. Suena ya a tópico recurrente decir que una Comisión

Europea entrante en una legislatura se enfrenta a la última oportunidad para que la Unión cierre (o cuando menos reduzca) la brecha tecnológica con Estados Unidos, y ahora también con China. Quizá por ello es más necesario que nunca en la Unión, y más en el área digital, se afronte "un cambio radical".

4.2. COCINA ITALIANA PARA RECUPERAR EL LUGAR DE EUROPA EN EL ESCENARIO GLOBAL

4.2.1. Dos informes clave: Letta y Draghi al rescate de Europa

Cuando restaba un año para la conclusión del mandato de la primera Comisión presidida por Ursula Von der Leyen, la necesidad de un giro estratégico en la política europea se hizo evidente. Tras el shock de la pandemia de la COVID-19, el retorno a la normalidad económica en la UE estaba siendo de una debilidad manifiesta comparada con la de las otras dos grandes áreas económicas. Ya hemos avanzado que la brecha del PIB entre EE. UU. y la UE se había ampliado, llegando a duplicarse en términos absolutos entre 2018 y 2023, pero también se perdía terreno respecto de la economía china que pugnaba por realizar el *sorpasso* de la europea (ver **figura 4.1**).

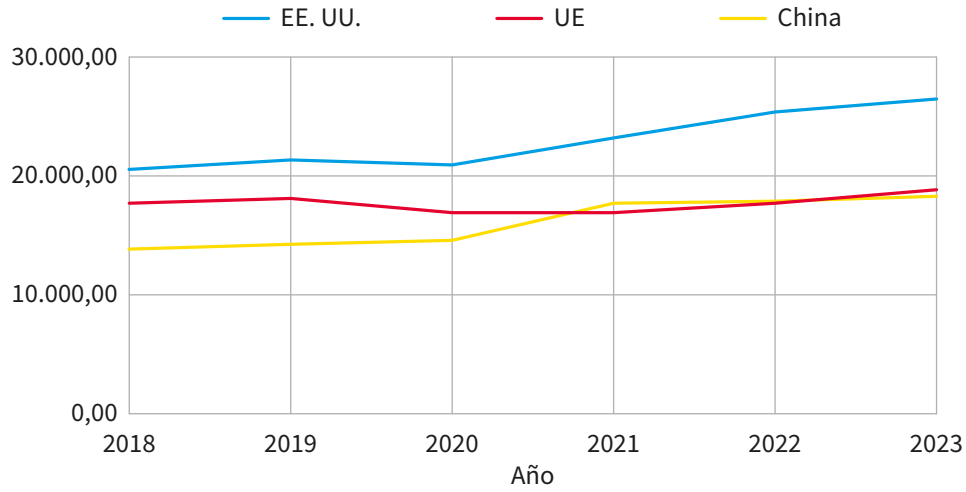


Figura 4.1.
Evolución del PIB de EE. UU., UE y China (unidades billones de dólares estadounidenses) (9).

La mayor dependencia del turismo, la guerra de Ucrania y la crisis energética estaban dando lugar a una recuperación pospandémica excesivamente lenta de la economía europea, en la que si bien se consiguieron controlar de un modo rápido las tensiones inflacionistas otros indicadores no presentaban un panorama alentador. Además de la lenta recuperación del crecimiento del PIB, la productividad se incrementaba a un ritmo superior fuera de Europa.

En dos de las tres instituciones centrales de la gobernanza de la Unión Europea, la Comisión Europea y el Consejo Europeo, las alarmas se encendieron y recurrieron a asesoramiento externo en la búsqueda de soluciones.

En primer lugar, en su reunión de junio de 2023, los líderes políticos de los estados miembros pidieron que se les presentara, en su reunión de marzo de 2024, un informe independiente de alto nivel sobre el futuro del mercado único

(10). Unos meses más tarde, la elaboración del documento fue encomendada a Enrico Letta, presidente del Instituto Jacques Delors, de común acuerdo entre los Gobiernos de España y Bélgica, los dos países que iban a ostentar la presidencia rotatoria del Consejo de la UE en el plazo dado por los líderes para completarlo.

El dossier "Mucho más que un mercado" elaborado por Enrico Letta fue finalmente presentado al Consejo en abril de 2024 (11). La principal conclusión del informe elaborado por el político italiano es la necesidad de adaptar el mercado único al nuevo contexto geopolítico, económico y social, muy diferente al del momento en que surgió. En particular, dentro del ámbito tecnológico, Letta incidía en la necesidad de profundizar en el mercado único de las telecomunicaciones y favorecer la inversión privada en la transición digital, dando forma al mercado único de capitales. Si bien el político italiano destacaba el valor del mercado único como el arma más potente de la economía europea, consideraba que su efectividad como herramienta para desarrollar la autonomía estratégica e impulsar el crecimiento quedaba en entredicho si no se ponían en marcha reformas inmediatas.

Por su parte, la presidenta de la Comisión Europea anunció en la edición del debate sobre el Estado de la Unión de septiembre de 2023 que había encomendado a Mario Draghi la elaboración de un informe sobre el futuro de la competitividad europea (5) (6). Si bien se esperaba que el documento estuviera concluido inmediatamente después de las elecciones al Parlamento de la Unión Europea celebradas en junio de 2024, su presentación se demoraría unas semanas más, no realizándose hasta el 9 de septiembre.

Mario Draghi dividió su informe "El futuro de la competitividad europea" en dos volúmenes. Uno primero de carácter general, "Una estrategia de competitividad para Europa", y otro de análisis de sectores clave en el desarrollo de la estrategia, "Análisis en profundidad y recomendaciones". El político identificaba en su estrategia tres áreas clave para que la UE recuperará el ritmo de crecimiento que había tenido en el pasado: cerrar la brecha de innovación con EE. UU. y China (especialmente en tecnologías avanzadas), un plan conjunto para la descarbonización y la competitividad y aumentar la seguridad y reducir las dependencias.

Se trata, en definitiva, de dos informes complementarios, pero en ambos la digitalización es vista como un pilar central para un retorno de Europa a la senda del crecimiento, imprescindible para mantener su sociedad del bienestar. También los documentos de ambos políticos italianos coinciden en su análisis del contexto global, dibujando dos áreas económicas en fuerte rivalidad, EE. UU. y China, entre las que Europa ha de encontrar un lugar. En la pugna entre las dos potencias la batalla tecnológica es central, y consecuentemente será clave para Europa desarrollar políticas públicas que promuevan su autonomía digital estratégica de modo efectivo y real. En sus propuestas, Letta y Draghi no solo abogan como objetivo para Europa ser competitiva en el área digital sino porque la digitalización sea el motor de la competitividad, un objetivo que sintetizaba Raquel Jorge (12).

4.2.2. Las infraestructuras digitales y tecnologías críticas: diagnóstico y recomendaciones

La construcción de la autonomía digital estratégica en el medio plazo depende de las estrategias y apuestas de hoy. Hemos anticipado los componentes que la Comisión Europea considera que han de ser el centro de las políticas públicas digitales —telecomunicaciones y tecnologías digitales críticas—. Draghi y Letta respaldan en sus informes la selección de áreas realizada y desarrollan recomendaciones sobre las estrategias a seguir en cada una de ellas.

Las infraestructuras son un elemento fundacional de la transición digital y pilar de la autonomía estratégica. La Unión Europea había dispuesto siempre de una posición adelantada en este ámbito respecto a EE. UU., pero comenzó a rezagarse con el despliegue

de 4G. De acuerdo con el informe de Analysys Mason publicado en 2025, la situación no ha mejorado para Europa con el despliegue de las últimas generaciones de redes fija y móvil. Mientras en EE. UU. la cobertura de 5G alcanza ya el 98 % en la Unión se encuentra en un 87 %, con una brecha superlativa si nos focalizamos solo en 5G *stand-alone* donde las coberturas son, respectivamente, 91 % y 40 %. Por su lado, las redes fijas preparadas para velocidades de acceso de 1 Gbps en EE. UU. cubren el 90,3 % de la población y en Europa el 82,5 %. Los datos comparativos respecto a China no son mejores, en el gigante asiático el 90 % de la población tiene cobertura 5G y el 99 % conectividad gigabit en sus hogares (8).

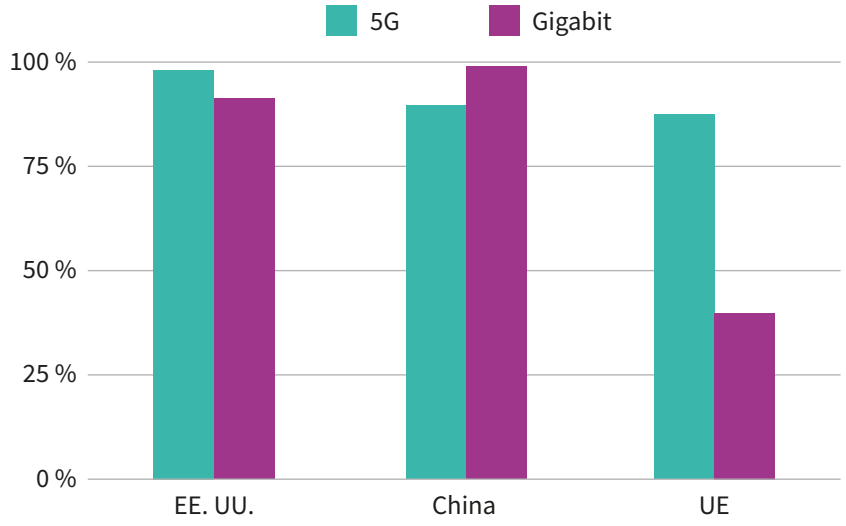


Figura 4.2.
Cobertura poblacional de 5G y acceso gigabit en EE. UU., China y la UE (7).

Para revertir la situación, como hemos comentado, es necesario un inmenso esfuerzo inversor, pero también una reforma profunda del mercado de las telecomunicaciones europeo. El informe anual de Analysys Mason refleja la gran fragmentación del sector en Europa (más de 41 operadores móviles europeos con más de 500.000 abonados frente a 5 en EE. UU. y 4 en China), lo que desemboca en una extremada debilidad financiera de sus operadores (bajo ARPU, declive en ROCE y dramática reducción del valor bursátil). La consecuencia es que el *capex* per cápita de los operadores de telecomunicaciones europeos es sensiblemente inferior al de los estadounidenses —226,4 € vs 177,9 €— y sin perspectivas de potencial aumento. La conclusión es obvia desde hace tiempo para la industria: la necesidad de consolidación transnacional de operadores dentro de un mercado único de telecomunicaciones.

Después del fracaso del esfuerzo reformista de 2023, la Comisión Europea publicó en febrero de 2024 el Libro blanco "¿Cómo abordar las necesidades de infraestructura digital de Europa?" (13). En el documento se analizan los desafíos que enfrenta actualmente el Viejo Continente en el despliegue de futuras redes de conectividad y presenta posibles escenarios para atraer inversiones, fomentar la innovación, aumentar la seguridad y lograr un verdadero mercado único digital. También Enrico Letta y Mario Draghi presentan la reforma del sector de las telecomunicaciones en la UE y el avance hacia un mercado único en este ámbito como una de las tareas que Europa ha de abordar de modo perentorio.

Pero no solo se trata de disponer de unas redes de acceso ubicuas y que permitan a ciudadanía y empresas acceder a los beneficios de la digitalización de modo pleno. Las crisis geopolíticas han hecho aflorar la dependencia de la autonomía digital estratégica de infraestructuras digitales extraterritoriales, como los cables submarinos por los que transcurren diariamente operaciones financieras valoradas en 10 billones de dólares (14), las redes satelitales de órbita baja que han jugado un rol central en la guerra de Ucrania y los centros de servicios en la nube que

soportan, entre otras, las aplicaciones de IA. En todos estos casos, la UE no solo está quedando también detrás respecto de EE. UU., sino que se están generando nuevas dependencias respecto de las grandes tecnológicas estadounidenses: Amazon, Google, Microsoft y Meta se han configurado como grandes operadores de conectividad oceánica habiendo puesto en marcha una cuarta parte de los sistemas que comenzaron a operar entre 2019 y 2023 (14); Starlink domina de modo incontestable las comunicaciones desde el espacio con un 60 % de los satélites en órbita; y Amazon, Microsoft y Google acumulan el 80 % del mercado europeo de la nube.

Los argumentos y escenarios para la reforma del mercado de telecomunicaciones presentados por la Comisión y los políticos italianos son similares. En particular, se hace una priorización de una expansión competencial de la Comisión difícilmente admisible por los estados miembros (refuerzo del papel en la gestión del espectro, autorizaciones centralizadas, productos mayoristas únicos, …). De igual modo presentan una opción dulcificada del *fair share*, basada en un acuerdo mutuo entre operadores y las grandes tecnológicas, y la necesidad de una cierta convergencia regulatoria entre redes y la nube. La reacción de los estados miembros ha vuelto a ser reticente a una reforma en estos términos, como reflejó el documento de Conclusiones del Consejo aprobadas en diciembre de 2024 (15). Es más, incluso los Gobiernos europeos acusaron de "falta de material analítico que respalde algunas de las conclusiones que se hacen en el Libro Blanco y en el informe Draghi".

Junto con las infraestructuras digitales, la Comisión Europea saliente recomendó considerar como tecnologías críticas aquellas que cumplen con al menos tres criterios: la naturaleza habilitadora y transformadora de la tecnología; el riesgo de fusión civil y militar; y el riesgo de mal uso de la tecnología para violaciones de derechos humanos (4). Es decir, aquellas que en mayor o menor medida tenían carácter transversal de aplicación en varios sectores y cuyo uso disruptivo puede suponer un riesgo. Dando un paso más, identificó un número de ellas y las agrupó en diez categorías, entre las que destacó cuatro grupos que presentan los riesgos más sensibles e inmediatos relacionados con la seguridad tecnológica de la UE. Como hemos señalado ya, tres de estos grupos especialmente relevantes entre las tecnologías críticas tienen impacto directo sobre la autonomía digital estratégica de la Unión: los semiconductores, la inteligencia artificial (IA) y la tecnología cuántica.

En la Brújula Digital, la UE se marcó objetivos en estos tres ámbitos de las tecnologías críticas. En primer lugar, alcanzar el 20 % de la producción mundial de semiconductores en el año 2030; en segundo lugar, disponer en 2025 del primer ordenador europeo con aceleración cuántica; y, en tercer lugar, promover la adopción de la inteligencia artificial por el 75 % de las empresas europeas antes de 2030 dedicando más de 20.000 millones de inversión en diez años antes de 2030. En todas estas áreas tecnológicas, la Comisión Von der Leyen 1.0 había desplegado estrategias que habrá de culminar la Comisión Von der Leyen 2.0, pero sobre las que han existido algunas críticas. El ex presidente del Banco Central Europeo realiza recomendaciones en el volumen de análisis sectorial sobre las carencias para la competitividad de Europa en estas áreas.

En primer lugar, la IA es vista por el político italiano como una oportunidad para los actores industriales de la UE, pero como un riesgo dada la débil posición de Europa en este ámbito, sin proveedores tecnológicos fuertes en *hardware* o *software*. Sitúa el epicentro de la debilidad en un fuerte déficit inversor de la UE en esta tecnología. Solo la inversión en IA de las cuatro mayores empresas tecnológicas estadounidenses (alrededor de 200.000 millones de euros en 2024) supera todo el presupuesto anual de la UE (170.000 millones de euros al año) (16).

Más optimista es el político italiano al respecto de la situación de la Unión en la carrera de las tecnologías cuánticas. Europa cuenta con puntos fuertes clave en esta área —una gran inversión pública, excelentes capacidades de I+D y capital humano— aunque está lastrada por la falta de interés del sector privado por esta área.

Finalmente, Draghi es moderadamente crítico con las ganancias recogidas por el ecosistema de semiconductores de Europa con la Ley de Chips, sobre todo considerando que las inversiones finales atraídas el multiplicador de la inversión pública en la UE ha sido sensiblemente inferior al de EE. UU. (ver **tabla 4.1**). Además de la consabida necesidad de mayores inversiones, el economista llama en su informe a recalibrar las ambiciones y necesidades de la UE en esta área y a construir un liderazgo claro que integre las decisiones en este campo de políticas públicas.

Tabla 4.1. Evaluación preliminar de resultados de estrategias para desarrollo de industrias de semiconductores en las distintas áreas económicas (17).

Región	EE. UU.	China	UE	Japón	Corea del Sur	Taiwán
Principales incentivos (millones de dólares)	39.000	142.000	47.000	17.500	55.000	16.000
Tipo incentivo	Subvenciones	Fondos de capital	Subvenciones	Subvenciones	Incentivos fiscales	Incentivos fiscales
Número de inversiones en líneas de fabricación desde 2020	26	30	8	4	3	7
***Capex* en cada región previsto entre 2024 y 2032 (millones de dólares)**	646.000	157.000	156.000	222.000	300.000	716.000
% Incremento capacidad producción (wspm)	203 %	86 %	124 %	86 %	129 %	97 %

También los estados miembros, en la sesión del Consejo de la Unión celebrada en diciembre de 2024, señalaron que, de modo general, para alcanzar sus metas y objetivos tecnológicos de aquí a 2030 la UE debería reevaluar sus objetivos de la década digital en 2026. Existe una conciencia de la necesidad de redoblar esfuerzos para reflejar el ritmo acelerado de los recientes avances tecnológicos si la UE no quiere seguir perdiendo terreno frente EE. UU. y China en las tecnologías críticas, en particular en la IA.

Finalmente, la todopoderosa Comisión de Industria, Investigación y Energía (ITRE) del Parlamento europeo está elaborando el informe "Soberanía tecnológica europea e infraestructura digital" (18). El objetivo del documento es identificar las brechas y las oportunidades para que Europa sea menos dependiente de la tecnología desarrollada en otras áreas económicas. Se espera que abarque la conectividad, la inteligencia artificial y la computación cuántica, y que formule recomendaciones para iniciativas de regulación e inversión. El Parlamento espera esté disponible en septiembre de 2025 para poder influir en las propuestas legislativas y estratégicas que la nueva Comisión Europea está preparando.

Draghi, Letta, la Comisión Europea, los estados miembros, Parlamento de la Unión… Existe un consenso en el diagnóstico sobre qué áreas tecnológicas han de priorizar las políticas públicas europeas para potenciar su autonomía digital estratégica. Se trata, en definitiva, de ser capaces de construir un "Eurostack" que aborde las dependencias en los ámbitos tecnológicos críticos: desde los microchips y los centros de datos hasta los servicios en la nube, los espacios de datos y la IA. Como diagnosticaba Manuel Hidalgo, "innovar más, digitalizar más, descarbonizar más. Pero entre el diagnóstico y la acción se alza un muro de contradicciones internas" (19). Las fórmulas y recetas para ello serán el campo de disputa en la legislatura que se abre, pero el pilar del mercado único no puede dejar de ser un elemento central.

4.2.3. Las palancas del mercado único para el desarrollo de la autonomía digital estratégica

El mercado único es, al mismo tiempo, la piedra angular de la integración europea y su arma geopolítica de mayor potencia. El Parlamento europeo estima que dentro de las fronteras de la Unión Europea conviven 449 millones de consumidores y 31 millones de empresas activas, la mayoría de las cuales son pequeñas y medianas empresas. También atribuye de modo directo al mercado único el 8 % y el 9 % del Producto Interior Bruto (PIB) de la Unión Europea y 56 millones de puestos de trabajo (20). Los informes elaborados por Enrico Letta y Mario Draghi coinciden en la necesidad de profundizar en su desarrollo, proponiendo reformas de calado cuya implementación haría posible una mayor autonomía digital estratégica de la Unión.

Existe una coincidencia entre ambos políticos italianos en la necesidad de inversiones masivas para alcanzar los objetivos políticos de la Unión, que Mario Draghi cifra en 800.000 millones de euros anuales. La digitalización de la Unión es uno de los focos centrales de absorción de dichas inversiones, en cuya necesidad coinciden personas situadas en las antípodas políticas del italiano como Yannis Varoufakis —que apunta que si no existe en Europa un Amazon o un Meta es por falta de inversión—. La Comisión Europea estimó en el año 2021 que para reducir la brecha tecnológica con Estados Unidos se necesitaría una inversión de 125.000 millones de euros al año (21), y más adelante, en 2023, apuntó que los estados miembros deberían dedicar un 3 % de su PIB al I+D en tecnología digital (22).

Las elevadas necesidades de inversión para dar cabida a la transición digital entre los objetivos estratégicos de la Unión deberán ser satisfechas tanto por el sector privado como por el público. Consecuentemente con esta visión, Letta y Draghi realizan propuestas en los dos sentidos. Por un lado, completar la unión del mercado de capitales (UMC) con una unidad de mercado de ahorros e inversiones, garantizando que las empresas obtengan condiciones de financiación comparables independientemente del estado miembro en el que estén ubicadas. Por otro, habilitando endeudamiento común para financiar bienes públicos europeos, que incluirían las infraestructuras digitales, de modo similar a como se hizo con el Mecanismo de Recuperación y Resiliencia (MRR) pospandemia.

Ambas reformas son necesarias pero complejas de ejecutar. La profundización en la UMC es calificada por algunos analistas como una medida limitada, que puede ser insuficiente para movilizar hacia la inversión productiva el 34,1 % de ahorros europeos en depósito bancarios que identifica Letta. El comportamiento de la inversión de los consumidores en Europa evita tradicionalmente las pérdidas en el corto plazo que pueden suponer proyectos tecnológicos disruptivos, siendo una barrera difícil de romper, una propuesta alternativa que los analistas consideran más viable es introducir medidas incentivadoras a la banca minorista para que inviertan los ingresos de manera más productiva. Por su parte, algunos de los estados miembros más pequeños, como Luxemburgo, Malta e Irlanda, son reacios a una supervisión más centralizada del mercado de capital.

Tampoco existe de momento escaso consenso para una reedición de las fórmulas de endeudamiento común utilizadas para la recuperación Europea tras la irrupción de la COVID-19. La Comisión propuso ya en la anterior legislatura desarrollar un ambicioso fondo soberano europeo que facilitara las inversiones en los ámbitos tecnológicos digitales frontera. La iniciativa constaba de una plataforma de tecnologías estratégicas para Europa (STEP), con intención de dotarla inicialmente con 10.000 millones de euros para seleccionar y ejecutar proyectos de interés común. Finalmente el acuerdo que alcanzaron Consejo y Parlamento en febrero de 2024 dejó STEP en un mecanismo proveedor de sellos de excelencia sin fondos nuevos añadidos (23). La urgencia de este fondo de soberanía tecnológica, que la nueva Comisión Europea ha vuelto a plantear como iniciativa, es mayor si cabe ahora, ya que la segunda administración Trump está planificando crear su propio instrumento de estas características.

Pero los dos políticos italianos no se quedan tan solo en propuestas para desatar la inversión privada y pública, también realizan propuestas para renovar uno de los instrumentos comunitarios que las condicionan: la normativa de ayudas de Estado. Ambos autores coinciden en la necesidad de adoptar una mayor aproximación hacia el bien común europeo, en particular, agilizando y flexibilizando el marco de concepción y aprobación de los proyectos comunes importantes de interés europeo (IPCEI, *Important Projects of Common European Interest*). No faltan razones para ello con experiencias previas como el IPCEI de semiconductores, que tardó más de dos años en gestarse para generar un proyecto sin un fin claro más allá de regar de subvenciones el ecosistema sectorial europeo.

En definitiva, Enrico Letta y Mario Draghi no proponen algo muy diferente de la ya comentada circulación dual que ha facilitado el gran desarrollo tecnológico de China en los últimos años. Los políticos italianos ponen sobre la mesa las oportunidades no aprovechadas del mercado único y su potencial para usarlos como palanca del desarrollo digital de la Unión. Un impulso de la industria tecnológica que facilite la ruptura de dependencias y, consecuentemente, promover la autonomía digital estratégica europea.

4.3. TRUMP 2.0 Y DEEPSEEK: LA UE FRENTE A LOS NUEVOS CISNES NEGROS EN LA GEOPOLÍTICA DIGITAL

4.3.1. El renacer de los disensos entre EE. UU. y la UE

Tras una intensa campaña electoral en 2024, EE. UU. votó por el Partido Republicano. El resultado que trajeron las urnas no solo ha sido el comienzo de una segunda administración Trump, también dio lugar a un control sobre el legislativo para el partido del elefante azul, que ha recuperado la mayoría en el senado y la retiene en el congreso. El cambio de signo político en Washington trae una nueva agenda tecnológica a EE. UU. que parece conducir a una ruptura, o cuando menos enfriamiento, de la colaboración con la UE en ámbito digital.

En las primeras etapas del camino que recorrió el magnate neoyorquino para volver al Despacho Oval se identificó su agenda política con el informe del Proyecto 2025 (24), cuyo origen se remonta a los primeros meses de 2023. El proyecto estaba diseñado como una guía para la transición presidencial y la implementación de políticas neoconservadoras desde el primer día de la nueva administración. Aunque diversas fuentes negarán que el Proyecto 2025 fuera la plataforma ideológica para la reelección de Donald Trump —con especial vehemencia por American Heritage promotores del documento— lo cierto es que diversas figuras clave en su elaboración han sido elegidos para puestos de responsabilidad en el equipo inicial de la nueva administración republicana. No existe en el documento estratégico un apartado específico dedicado a la política tecnológica, pero pueden extraerse del mismo diversas ideas maestras a este respecto.

El Proyecto 2025 incluye algunas propuestas tecnológicas que es factible ejecute el nuevo Gobierno En primer lugar, una mayor centralización de las funciones de ciberseguridad en la Agencia de Seguridad Nacional (NSA) en detrimento de otras como la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA). En segundo lugar, una apuesta por impulsar las comunicaciones satelitales acelerando la concesión de licencias, la financiación y el proceso de revisión para los servicios basados en LEO (*Low Earth Orbit*) y apoyo a la innovación en este ámbito, algo coherente con el fuerte apoyo a Trump por parte de Elon Musk.

La agenda política de American Heritage también se centra en la rivalidad con China en la Inteligencia Artificial (IA), considerando crítico para asegurar el liderazgo que el gobierno invierta en innovación y la proteja, absteniéndose de intervenciones regulatorias para atajar

sus presuntos riesgos. De modo coherente con esta visión, Trump ha derogado la orden ejecutiva adoptada por Biden para el desarrollo seguro de la IA y ha adoptado una propia (25). De la orden ejecutiva aprobada por Trump ha de emanar en 180 días un plan de acción destinado a mantener y extender el dominio de EE. UU. en la IA, contando con los comentarios de las partes interesadas. Probablemente, el objetivo de un desarrollo seguro y de confianza de esta tecnología propugnado por la Ley de inteligencia artificial de la UE parece no entrar en la ecuación.

Puede sorprender actualmente que el Proyecto 2025 sea crítico con las grandes plataformas tecnológicas, aunque no debería hacerlo. El documento está elaborado por trumpistas de primera hora, con reticencias hacia los gigantes tecnológicos por su papel tras el asalto al Capitolio del 6 de enero de 2025. Recordemos que las empresas de redes sociales e internet se alinearon en su momento con los que pedían la censura digital de las opiniones que incitaban a la revuelta, incluyendo el cierre de las cuentas del presidente Trump. Consecuentemente, el marco estratégico oficioso del Partido Republicano señalaba la necesidad de una mayor regulación de los gigantes digitales, en concreto empoderando a los usuarios en filtrado de contenidos, imponiendo reglas de transparencia algorítmica en la distribución de información y estableciendo límites a las acciones contrarias (según su visión) a la libertad de expresión. También demandaban que, a las empresas de redes sociales, buscadores, comercio-e y video bajo demanda, entre otras, se les exigiera contribuir al fondo del servicio universal.

Tras el apoyo de los tecno oligarcas a Donald Trump, la implementación de las propuestas de American Heritage sobre plataformas digitales han entrado en una vía lenta e incierta, creando contradicciones en el seno del movimiento populista estadounidense. Es difícil identificar en este momento si la investigación abierta por la Federal Trade Commission (FTC) sobre la censura en las plataformas digitales en los últimos años tiene un afán persecutorio o exculpatorio de los tecno oligarcas, pero lo cierto es que todos ellos, menos Elon Musk, tuvieron responsabilidad en una era identificada como negra para la libertad de expresión por parte del Partido Republicano. Lo que por ahora es cierto es que la nueva Administración desarrolla una política proteccionista hacia las plataformas digitales que ya ha comenzado a crear tensiones con Europa y otros países, al considerar que los denominados impuestos digitales son una traba al libre comercio.

En su intervención en la cumbre de Davos el presidente estadounidense atacó a la UE por su estricta regulación sobre los gigantes digitales y las investigaciones de competencia abiertas sobre ellos. La fase de implementación efectiva de Digital Services Act (DSA) y Digital Market Act (DMA) en la que entra ahora la UE está teniendo enfrente a la Casa Blanca. La primera señal de aviso es el memorando presidencial "Defendiendo a las empresas y a los innovadores estadounidenses de la extorsión extranjera y de multas y sanciones injustas". El presidente Trump realiza en el mismo una amenaza clara a Europa de nuevos aranceles por sus políticas hacia los gigantes tecnológicos al señalar que "cuando un gobierno extranjero, a través de su estructura fiscal o regulatoria, imponga una multa, sanción, impuesto u otra carga que sea discriminatoria, desproporcionada o diseñada para transferir fondos significativos o propiedad intelectual, mi Administración actuará" (26). Las amenazas se redoblaron en el proceso de negociación de los llamados aranceles recíprocos a partir de abril de 2025.

La confrontación regulatoria entre EE. UU. y la UE guiada por los intereses de las grandes tecnológicas, se extenderá más allá de las investigaciones de mercado y la implementación de DSA y DMA. Es probable que la Comisión proponga en la propuesta de Ley de Redes Digitales (*Digital Network Act*, DNA) preceptos encaminados a la convergencia regulatoria entre las infraestructuras de red y de la nube. Es previsible también que incluya en su articulado la llamada distribución justa de costes de las redes —*fairshare*— destinada a que las grandes plataformas digitales contribuyan a las necesidades de inversión en redes europeas. A pesar de las reticencias de algunos estados miembros, la Comisión Europea está ahora respaldada para

realizar estas proposiciones por las recomendaciones del informe de Mario Draghi. Las grandes tecnológicas estadounidenses, vistiéndose como abanderadas del "America First" trumpista, buscarán frenar estas intenciones atrayendo al inquilino de la Casa Blanca hacia su causa contra el afán regulatorio bruselense.

Finalmente, no solo los disensos regulatorios están renaciendo, sino que está en riesgo de desaparecer la mesa de diálogo donde EE. UU. y la UE tendían puentes entre sus diferentes visiones sobre el mundo digital. De igual modo que en su primer mandato, Trump parece negar a la UE el papel de interlocución, promoviendo relaciones bilaterales con los estados miembros, en especial con aquellos en que su dirigencia mantiene coincidencias ideológicas. Nada hace prever un interés de la segunda Administración Trump por mantener las reuniones del Consejo de Comercio y Tecnología, dando fin a la institucionalización de la cooperación tecnológica. Parafraseando a Jean Claude Juncker, también en el ámbito digital, "Trump nos obliga a los europeos a poner nuestro destino en nuestras manos".

4.3.2. DeepSeek: una enmienda a los modelos de gobernanza digital

Apenas constituida la segunda Administración Trump otro evento conmovió los cimientos de la geopolítica digital. Un laboratorio tecnológico chino hasta entonces desconocido, DeepSeek, hacía público un modelo de inteligencia artificial equivalente o cercano a los más avanzados desarrollados por la industria estadounidense. El hito se interpretó inicialmente como el último episodio de la rivalidad tecnológica. Desde 2022, las empresas de IA localizadas en China tenían restringido el acceso a los chips más avanzados por las regulaciones comerciales estadounidenses, lo que les había obligado a buscar el progreso en innovaciones algorítmicas como aquellas con las que DeepSeek estaba asombrando al mundo.

Está fuera del ámbito de este texto la evaluación tecnológica del logro de la empresa china. Han corrido ríos de tinta y de bits tanto alabando como minusvalorando el hito, pero la *startup* china es más que la cuna de un modelo de aprendizaje altamente creativo que demuestra que la guerra tecnológica está lejos de concluir. La existencia de DeepSeek supone también un cuestionamiento simultáneo a los modelos de desarrollo digital propugnados por las tres grandes áreas económicas.

Existen indicios que los medios oficiales de la República Popular de China fueron relevantes amplificando las narrativas relativas al reto que el modelo de DeepSeek al dominio estadounidense en la IA (27). El triunfalismo oficial ocultaba que su empresa matriz —High Flyer— había sufrido en su día la persecución del oficialismo hacia los fondos cuantitativos de inversión libre (*quant hedge fund*) y que el éxito de su filial tecnológica no se había construido sobre los pilares tradicionales del modelo de gobernanza digital chino.

DeepSeek representa una ruptura, al menos parcial, con estos patrones predominantes en el sistema de innovación chino. La *startup*, fundada en 2023 como laboratorio de un fondo cuantitativo de inversión libre, se diferencia del panorama tecnológico chino altamente competitivo por su cultura laboral y organizativa, liderazgo, financiación en gran parte estatal y formación de su capital humano. A diferencia de los gigantes tecnológicos chinos —Tencent, Alibaba, etc.— que imitan los modelos de Silicon Valley, la joven empresa china no promueve largas jornadas de trabajo y su fundador no proviene de la nomenclatura del Partido Comunista Chino (PCCh). Además, la *startup* IA ha sido financiada íntegramente por High-Flyer, sin apoyo estatal, y su equipo cuenta con formación mayoritariamente china, incluyendo a sus profesores (28).

En EE. UU. las reacciones tras la aparición de DeepSeek apuntan hacia la quiebra definitiva de la creencia en un modelo de libre mercado sin condicionantes políticos como conductor de la digitalización mundial. La élite dirigente estadounidense había comenzado a virar hacia una ruptura con un marco de competencia

abierta en el ámbito digital tras el final de la presidencia de Barack Obama. Muestras del nuevo consenso bipartisano desde 2016 son la ofensiva durante la primera presidencia de Trump para expulsar a Huawei de las infraestructuras 5G en occidente y las restricciones a las exportaciones en semiconductores a China impuestas por la Administración de Biden. La emergencia de DeepSeek ha agudizado la tendencia hacia el embridamiento de las empresas tecnológicas estadounidenses por el poder político, estableciendo límites aún más estrechos a su libre participación en el mercado global. El Comité Selecto del PCCh del Congreso de EE. UU. propuso reforzar y extender los controles de exportación a los productos IA de Nvidia usados por DeepSeek (29), aunque dañase el negocio de la empresa californiana. Por su parte, Howard Lutnick, en la audiencia que le confirmó como secretario de Comercio, señaló que las empresas estadounidenses debían dejar de facilitar a las compañías chinas las herramientas para ser tecnológicamente competitivas.

Si DeepSeek cuestionaba en China la efectividad del modelo estatalista como la vía para disponer de un ecosistema digital competitivo y en EE. UU. reforzaba al poder político en la creencia de limitar la libertad de mercado a sus empresas tecnológicas, en la clase dirigente europea elevó las dudas sobre el "efecto Bruselas". La UE había proclamado a los cuatro vientos su éxito en ser la primera área económica en dotarse de una regulación para un desarrollo seguro de la IA, al mismo tiempo que soñaban que los productos de alguna *startup* comunitaria como Mistral igualara a los del ecosistema estadounidense.

Todo apunta que el afán de Europa por marcar las leyes de la esfera digital no va a tener el mismo éxito a partir de ahora y que la IA es el primer ámbito en que se está manifestando. Por un lado, los gigantes digitales, lejos de expresar el deseo de extender la aplicación de la Ley IA a otras jurisdicciones como hicieron con el Reglamento de Protección de Datos, se mostraron reticentes a comercializar sus servicios IA en la UE —Apple, Meta—. Por otro lado, la esperanza de extender el marco legal a EE. UU. se vio frustrada por la ya comentada anulación exprés por Trump de la orden para una IA segura aprobada por Biden. También desde China se aconseja prudencia regulatoria en este momento y evitar ahogar la innovación (30). El fracaso en generar una alternativa europea similar a DeepSeek es un recordatorio para la Unión de que su capacidad futura de fijar los estándares regulatorios requiere de un modelo industrial del que hoy carece.

En conclusión, DeepSeek está poniendo de manifiesto las limitaciones de los modelos de desarrollo tecnológico existentes en China, Estados Unidos y la Unión Europea, presentando nuevos desafíos a sus estrategias. Las rendijas en el control absoluto del mercado interior de la nomenclatura china habían dado lugar a innovaciones claves para la soberanía tecnológica, el beneficio de las fuerzas de mercado dejaba de ser el único faro en EE. UU. y la ambición regulatoria europea necesita de un sistema industrial fuerte que apoye sus estándares normativos.

Los principios para la gobernanza digital seguidos hasta ahora por las tres grandes áreas económicas no permitirán un camino en la vuelta al multilateralismo digital. China parece haber interpretado que el caso DeepSeek le demanda potenciar el papel de su sector privado frente al del Estado en el ámbito digital, apoyándose en el mismo para un desarrollo digital basado en sus propios estándares. Xi Jinping mantuvo en febrero de 2025 una infrecuente reunión con las compañías tecnológicas reconociendo así su relevancia para rivalizar con EE. UU. y comprometiéndose a potenciarlos con una nueva Ley de Promoción Económica (31). Por su parte, en el mismo mes, durante la intervención del vicepresidente JD Vance en la cumbre de inteligencia artificial de París reafirmó la intención del Gobierno de EE. UU. de limitar a quienes comercializan la tecnología más avanzada que desarrollan sus empresas. La respuesta europea ha de ser impulsar la vuelta un entorno multilateral y abierto, pero con una nueva política tecnológica menos confiada en la viabilidad de un imperialismo regulatorio.

4.3.3. La UE como motor de la vuelta al multilateralismo

La UE empieza a asumir que la presidencia de Donald Trump supone un giro radical en el modelo de relaciones con EE. UU. Lejos de dañar su autonomía digital estratégica la nueva situación puede ser una palanca para su refuerzo. La UE tiene la ocasión de ser activa en la ruptura del escenario naciente de enfrentamiento bipolar económico y digital entre G7 y BRICS+, con EE. UU. y China de líderes respectivos. Forzada por las circunstancias, Europa puede recuperar su papel de árbitro entre las visiones de la transformación digital de los dos gigantes tecnológicos y su progresivo ensimismamiento. En la cumbre de Davos de 2025, Ursula Von der Leyen dio las primeras señales sobre la intención de Bruselas de jugar ese papel al declarar la intención de "profundizar la relación con China y, cuando sea posible, incluso ampliar nuestros lazos comerciales y de inversión".

En el nuevo escenario, Europa puede, y quizás debe, intervenir realizando la labor de pivote central del balancín entre las distintas visiones de la digitalización de China y EE. UU. No es una función nueva para la Unión, que ya desarrolla tradicionalmente, por ejemplo, en los foros de debate sobre la gobernanza de Internet. Por un lado, confrontando la visión de China, la UE ha defendido una Internet abierta, libre y no fragmentada que siga siendo una red de redes única y descentralizada, protegida de la injerencia política y control por parte de los gobiernos, donde se deben respetar principios fundamentales como los derechos humanos, la libertad de expresión y la privacidad. Pero al mismo tiempo, en contraste con EE. UU., Europa ha impulsado que exista un espacio para la regulación que facilite un espacio digital más seguro en el que los derechos fundamentales de los usuarios y las empresas puedan competir en igualdad de condiciones.

Aún en un tablero donde los principios de la gobernanza tecnológica están en evolución por la disrupción de la inteligencia artificial, Europa sigue siendo el camino intermedio hacia un mercado digital más abierto entre los dos grandes imperios geopolíticos. Pero Europa no puede por sí sola conducir la vuelta al multilateralismo digital, haciendo frente tanto al neoproteccionismo estadounidense como al expansionismo autosuficiente chino en la esfera digital. Es central para este fin reforzar las alianzas tecnológicas con otras áreas económicas. Las actuaciones en la pasada legislatura europea proporcionan una base para ello. En el marco de la estrategia de la Brújula Digital, se establecieron partenariados tecnológicos con Japón, Corea del Sur e India que revelarán su utilidad real en el nuevo escenario.

Con los mimbres descritos puede constituirse alrededor de Europa un bloque de potencias digitales de tamaño medio, con un mismo interés en romper la tendencia bipolar, particularmente en un escenario con una política arancelaria exacerbada por parte de Estados Unidos. Ese es el camino al que apunta la Estrategia Digital Internacional de la UE (32), adoptada en junio de 2025. La acción exterior de Europa en el ámbito digital, se centra en impulsar la competitividad europea promoviendo una agenda digital y gobernanza digital global. Su objetivo es fortalecer las alianzas internacionales, implementar una oferta comercial tecnológica europea y mejorar la gobernanza digital global basándose en valores fundamentales.

El papel de Europa como motor de la vuelta al multilateralismo, de tanta importancia en la esfera digital, ha sido también puesto de relevancia por otras personas con peso político relevante en la Unión. La presidenta del Banco Europeo de Inversiones (BEI), Nadia Calviño, aprovechó el foro de Davos para señalar que Europa debe "aprovechar la oportunidad para seguir profundizando sus relaciones estratégicas con otras partes del mundo" y de este modo tener una voz fuerte que contribuya a reforzar las instituciones multilaterales.

El recuerdo de la política comercial e internacional de carácter transaccional de Trump en su primera Administración puede favorecer una coordinación entre Europa y el resto de los socios tradicionales de EE. UU. Fue aquella una estrategia a la que no fue inmune el ámbito digital. Basta rememorar las actuaciones de la

Administración Trump en 2018 en su ofensiva por expulsar a Huawei de las redes 5G, sin margen de grises entre el conmigo o contra mí, o la imposición a TSMC de la prohibición de ventas de chips avanzados para los teléfonos de Huawei —entonces su segundo cliente— si quería seguir utilizando la tecnología estadounidense en sus procesos de fabricación. El camino hacia una alianza promultilateralismo digital liderada por la UE es largo, pero las continuas amenazas de la segunda Administración Trump amenazando continuamente con elevar los aranceles de socios tradicionales puede acelerar los plazos. Europa, como tercera potencia en el escenario global, se enfrenta a una oportunidad histórica.

4.4. URSULA 2.0: EL NUEVO CICLO DIGITAL POLÍTICO EUROPEO

4.4.1. Diagnóstico de una autonomía digital estratégica débil: una gobernanza digital regulatoria sin un centro de gravedad

El modelo de gobernanza digital europeo es criticado de modo recurrente por su exceso regulatorio. Son varios millares de páginas de nuevas regulaciones con influencia en el ámbito digital que han aprobado las instituciones europeas, en particular desde el año 2014 en que la Comisión Juncker adoptó la estrategia del Mercado Único Digital. Europa confío a la regulación la reducción de su brecha tecnológica con EE. UU. y de su dependencia tecnológica de este país. La UE dirigió sus esfuerzos en política digital a crear un acervo de normas comunes a los estados miembros en la creencia que la armonización liberaría su potencial tecnológico. Unas regulaciones en las que además se confiaba para tener influencia en el mercado global —por su aplicabilidad a las entidades que prestaban servicios en la UE aunque estuvieran localizadas en otra área económica— y que pretendía exportar como estándares al resto de territorios en una suerte de imperialismo regulatorio.

Hay quien señala que el mero exceso regulatorio ha estrangulado la innovación en Europa, siendo nombrado como principal causa de la falta de empresas europeas relevantes en el ámbito digital, y como consecuencia de su limitada autonomía digital estratégica. Otros, como Judith Arnal, señalan que el problema mayor reside no en la cantidad de normas sino en la implementación práctica de las mismas, tanto por demoras excesivas en las decisiones de los órganos regulatorios paneuropeos como por la fragmentación de interpretación de las autoridades nacionales (33).

En esencia, se señala que la regulación europea y cómo se aplica es culpable que no haya empresas de primer nivel con sede en la Unión en campos importantes como los sistemas operativos, las búsquedas, las redes sociales, la nube, el comercio electrónico o la inteligencia artificial. Los escasos casos de éxito —Skype, Spotify, Booking— han trasladado su sede a EE. UU. o han sido adquiridos por empresas de ese país. Son varias las fuentes de datos que reflejan la falta de músculo empresarial europeo en la esfera digital.

Strand Consult ha realizado un análisis identificando las 317 principales empresas de Internet en el mundo (34). Las compañías con sede en la UE representan solo el 2 % del valor total del mercado mundial de Internet, solo 52 empresas y menos de 250.000 trabajadores. El año medio de fundación es 1999, lo que demuestra que se han fundado pocas o ninguna empresa de Internet de la UE desde 2015. Por el contrario, EE. UU. y China siguen creando nuevas empresas de Internet; por ejemplo, Trump Media, fundada en 2021, tiene una capitalización de mercado de 7.500 millones de dólares, una cantidad mayor que todas las empresas de Internet de la UE en la lista excepto tres.

Tabla 4.2. Empresas relevantes de Internet localizadas en EE. UU., China y UE (35).

	EE. UU.	China	UE	Resto mundo	Total
Número de compañías de Internet	134	39	52	92	317
Capitalización bursátil (miles de millones de dólares)	8.440	1.217	172	656	10.485
Número de empleados	2.295.604	1.152.731	247.133	494.633	4.190.101
Año medio de fundación de las compañías	2006	2009	1998	1999	2003

La propia Comisión Europea ha puesto en evidencia esta situación en sus acciones regulatorias. Entre los siete *gatekeepers* (guardianes de acceso a la esfera digital) inicialmente designados por el Ejecutivo de Bruselas en el primer paso de implementación de la DMA, ninguno de ellos tenía sus accionistas principales en el Viejo Continente. Estas empresas, identificadas por disponer de una posición de mercado en alguna plataforma básica que les confiere el poder de crear un cuello de botella en la economía digital, tenían todo el control financiero en EE. UU., excepto una con mayoría de capital chino.

Aunque los datos estadísticos sobre la carencia de gigantes europeos en el mercado digital global son irrefutables, no existe un acuerdo generalizado en que el exceso regulatorio de la UE sea la raíz de esta situación. Así, Anu Bradford (36), mantiene el efecto beneficioso que las normativas europeas han tenido sobre la privacidad, competencia y lucha contra mensajes de odio en el entorno digital, e invita a mirar a otro punto para identificar la causa de la creciente brecha digital de la UE con EE. UU. y China: la falta de una política industrial tecnológica netamente europea. Del mismo modo que Mario Draghi y Enrico Letta, señala hacia la falta de una gobernanza europea de la política de inversiones e innovación, con una priorización basada en criterios de la Unión y no de los estados miembros y dotada de los fondos suficientes.

La carencia de un liderazgo en la gobernanza tecnológica europea se refleja también en la escasa coordinación de la diplomacia digital de la Unión. Existe una responsabilidad difusa sobre la acción exterior europea en esta área, donde unas veces la iniciativa compete a cada estado miembro, generalmente, de acuerdo a sus intereses nacionales, y otras a la Comisión Europea, en ocasiones sin una participación de las otras instituciones en la preparación de las posiciones y escasa rendición de cuentas de los resultados. A ello hemos de sumar que algunas regulaciones (IA, chips, ciberseguridad, …) definen sus propios mecanismos de cooperación internacional o la cohesión débil entre las actuaciones por cada estado miembro bajo el paraguas de la iniciativa Global Gateway.

La dispersión de las actuaciones internacionales de la UE limita sus opciones de disponer de variedad de alianzas para el desarrollo de su autonomía digital estratégica, en particular con el Sur Global. No obstante, hace concebir esperanzas de un cambio en este ámbito la toma de conciencia de la situación por el Consejo. En sus Conclusiones de julio de 2022, los estados miembros apostaban por la necesidad de garantizar que la diplomacia digital se convierta en un componente central y una parte integral de la acción exterior de la UE (37).

En definitiva, en cierta medida el exceso regulatorio, aunque no en el grado que algunos presuponen, y por otra parte las características confederales de su gobernanza tienen un impacto cierto en el estado de autonomía digital estratégica de la UE y el papel que juega en el escenario geopolítico actual. El programa de la segunda Comisión Europea dirigida por Ursula Von Leyden, armado sobre los argumentos de los informes de Draghi y Letta tiene entre sus objetivos superar estas limitaciones.

4.4.2. La autonomía digital estratégica en la nueva Comisión Europea y su programa político

La política digital oficial de la UE sigue siendo en el momento de escribir estas líneas la Brújula Digital, adoptada en el año 2021. Se presentaba en el documento una serie de actuaciones y objetivos para el año 2030 que permitiera satisfacer la ambición europea de ser soberana digitalmente en un mundo abierto e interconectado. Aunque su límite temporal queda lejos, es de esperar una renovación del marco estratégico seguido en los últimos cinco años, en particular con la desaparición del ejecutivo comunitario de quienes fueron sus principales impulsores, Margaret Vestager y Thierry Breton. La nueva Comisión Europea está dando los primeros pasos para renovar su estrategia tecnológica.

La presidenta Ursula Von der Leyen comenzó a señalar la nueva ruta digital europea en su intervención de investidura ante el Parlamento de la Unión Europea para su segundo mandato y en el programa político asociado (38). En lo relativo a la autonomía digital estratégica de Europa, Von der Leyen deja traslucir una menor ambición regulatoria global y un mayor foco en el desarrollo de proyectos estratégicos, apoyados por nuevos instrumentos de inversión y agilización de la gobernanza institucional.

Son cuatro los aspectos relevantes dentro del ámbito geopolítico tecnológico que incluyó la política alemana en el avance del programa de la nueva Comisión. En primer lugar, apuntó hacia una atenuación de la ambición legislativa, concentrándose en la implementación y el cumplimiento de las normas digitales adoptadas durante el mandato anterior, en particular los reglamentos de mercados y servicios digitales, así como de inteligencia artificial. También anunció su intención de proponer la creación de un Fondo de Competitividad Europeo, en un nuevo intento de dotar a la Unión del Fondo de Soberanía Europea que fracasó en la anterior legislatura, pero contando con aportaciones privadas y no sólo públicas. En tercer lugar, una agilización y simplificación de la tramitación de los IPCEI, crítica para afrontar grandes proyectos transeuropeos digitales. Finalmente, la revisión de la Directiva de Compra Pública dando preferencia en la misma a productos europeos en sectores estratégicos, que favorecerá que las cadenas de suministro de las tecnologías centrales para la autonomía digital estratégica mantengan manufactura en el continente.

La continuación del interés de la presidenta por seguir impulsando la autonomía digital estratégica como un aspecto central de su actuación, también se dejó sentir en la configuración del colegio de comisarios y comisarias para su segundo mandato. Tanto la responsable del área de competencia, Teresa Ribera, como de políticas digitales, Henna Virkkunen, mantuvieron el rango de vicepresidentas de las personas que les antecedieron. También es relevante que en el título oficial de esta última figure la responsabilidad sobre la "soberanía tecnológica". Toda una declaración de intenciones sobre la intención de Europa de volver a erigirse como una potencia digital autónoma que tratase de tú a tú a China y EE. UU.

Cada una de las vicepresidentas recibió de Von der Leyen su respectiva carta de misión, donde les especificaba los informes de Draghi y Letta como punto de partida de las políticas públicas que esperaba que desarrollaran. A Teresa Ribera, le señalaba que esperaba de ella una reforma profunda de la política de competencia, que la presidenta considera central para la autonomía digital estratégica. Concretamente, una simplificación de las normas de ayudas de Estado y para la configuración de los IPCEIs, expandiendo el potencial ámbito de estos más allá de la innovación hacia sectores estratégicos. También apuntaba la necesidad de acelerar las investigaciones de competencia para ganar en efectividad, incluyendo las relativas al DMA. Un indicador de la confianza en la lógica regulatoria de la DMA para limitar el poder de mercado de los *gatekeepers* que deje espacio a nuevos competidores, idealmente europeos reforzando la autonomía digital estratégica del continente.

A Henna Vikkunenn, como máxima responsable de las políticas digitales, Von der Leyen

le demandaba en su carta de misión la tarea central establecer los activos esenciales para la soberanía tecnológica y la resiliencia de la Unión. Dentro de las tecnologías críticas, como no podía ser de otra manera, la solicitaba impulsar la inteligencia artificial, reforzar las actuaciones e inversiones en tecnologías fronteras como la computación cuántica y progresar en la implementación de la Ley de Chips. Además de colaborar con la vicepresidente Ribera en asegurar la implementación de DMA y DSA, le encomendaba el desarrollo de propuestas de dos normas: la largamente esperada Digital Networks Act para implementar la reforma del mercado de las telecomunicaciones europeas y una nueva Ley de desarrollo de la inteligencia artificial y la nube de la UE.

4.4.3. El norte de la Brújula de la competitividad europea apunta hacia la era digital

El tiempo juega en contra de que Europa mantenga su relevancia como potencia global, en particular en el ámbito digital, y la nueva Comisión es consciente de ello. El último día del mes de enero de 2025, el Ejecutivo de Bruselas presentó su primera gran estrategia del nuevo ciclo legislativo, "Una brújula de competitividad para la UE" (39), comenzando a desarrollar así el programa político presentado por su presidenta en julio de 2024. El documento presenta la hoja de ruta de las iniciativas centrales que la Comisión Europea pretende impulsar en los próximos años, haciendo ver en la misma la intención de materializar las recomendaciones del informe elaborado por Mario Draghi. Sin ir más lejos, los nombres de los tres ejes centrales de actuaciones de la Brújula son "robados" de las prioridades para Europa marcadas por el político italiano.

El primer eje de la Brújula de la Competitividad pone uno de sus focos en el ámbito digital como uno de los tres imperativos transformacionales para fortalecer la competitividad. La selección es coherente con un mundo donde la tecnología es cada vez más un vector de cambio geopolítico y seguridad económica. Bajo el epígrafe "Cerrando la brecha de innovación", la Comisión Europea desgrana diversas iniciativas, algunas de las cuáles ya ha empezado a desarrollar en el primer semestre de 2025. Entre las mismas recoge actuaciones en los ámbitos de infraestructuras y de las tecnologías críticas digitales. En las intenciones que desvela el Ejecutivo de Bruselas hay luces y sombras.

En el área de las infraestructuras de telecomunicaciones y la nube, el calendario de la Comisión Europea resulta decepcionante para la urgencia de la reforma, demandada ya desde hace varios años. Sorprende que, tras los largos debates y varias consultas públicas realizadas por la burocracia de Bruselas en la anterior legislatura, la propuesta de Ley de Redes Digitales (Digital Network Act, DNA) no vaya a ser presentada hasta el último trimestre de 2025. El miedo de la industria a una continuación del día de la marmota que mantiene hibernada la reforma del sector desde hace ya unos años asoma de nuevo. A pesar del ya comentado estado financiero del sector, la Comisión Europea mantiene impasible su calendario. Solo presentará su propuesta legislativa conjuntamente con el informe de evaluación de la implementación del Código Europeo de Comunicaciones Electrónicas que tiene obligación legal de elaborar.

Otra propuesta pendiente de la anterior legislatura con impacto en el ámbito de las telecomunicaciones ha tenido mayor priorización y ya se ha materializado. En junio de 2025 la Comisión Europea publicó su propuesta de Ley del Espacio (*Space Act*). La Ley Espacial de la UE creará un mercado único para las actividades espaciales, incluyendo las comunicaciones satelitales, lo que facilitará a las empresas, en particular a las empresas emergentes y las pymes, crecer y operar a través de las fronteras.

La IA ocupa una buena parte de este pilar de innovación de la Brújula de la Competitividad,

con actuaciones que se desplegarán el segundo semestre de 2025 y el primero de 2026. La hoja de ruta europea esbozada en la "Brújula de la Competitividad" se ha desarrollado ya en el "Plan de Acción para un Continente de IA" (40), conteniendo como hito el desarrollo de una estrategia de IA aplicada para la UE, que dote al continente de las infraestructuras de computación, de nube y de datos que requiere. Dentro de la misma incluiría la Ley de desarrollo de la inteligencia artificial y la nube (*Cloud and AI Development Act*) con objetivo de movilizar la iniciativa pública y privada para establecer nuevas megafábricas de IA especializadas en el entrenamiento de modelos de gran tamaño. Otra actuación prevista es la implantación de un centro de I+D fundamental de IA, denominado "CERN de IA" que desarrolle casos de uso verticales, en particular para la ciencia. Los expertos de los *think-tank* europeos estiman que para cada una de las iniciativas serían necesarias, al menos, 300.000 millones de euros y 100.000 millones de euros, respectivamente (41), mientras la Comisión Europea tan solo espera movilizar con sus actuaciones 200.000 millones por ahora, partiendo de un fondo público denominado InvestAI, financiado con 20.000 millones.

De acuerdo con las previsiones de la Brújula, también que los servicios de la Comisión Europea han publicado en julio de 2025 una nueva estrategia de tecnología cuántica orientada a trasladar el reconocido potencial científico europeo en este ámbito a productos comerciales, incluso contribuyendo a la hoja de ruta tecnológica europea en materia de armamento (42). La estrategia de tecnología cuántica avanza que en 2026 se propondrá una Quantum Act para promover la inversión y desarrollo del ecosistema. El planteamiento de la estrategia de tecnología cuántica europea abarca el espectro necesario, con una apuesta holística que abarque computación, comunicaciones e infraestructura de sensorización basada en esta tecnología.

La política tecnológica de la nueva Comisión Europea que deja vislumbrar la Brújula de la Competitividad tiene también un esperanzador aspecto práctico. Uno de sus objetivos es reiniciar el círculo virtuoso de innovación en Europa, para lo cual no solo es necesario destacar en las tecnologías del futuro, sino también invertir en su aplicación y difundirlas en las cadenas de valor. En particular, hace hincapié en la necesidad de que la aplicación de tecnologías e infraestructuras críticas se apliquen en las líneas de producción de automóviles, robótica, energías limpias, telecomunicaciones y espacio para mejorar la soberanía tecnológica y la competitividad. En definitiva, para recuperar la autonomía digital estratégica perdida.

Si llama la atención la ausencia en la Brújula de la Competitividad de actuaciones para rectificar la estrategia europea en semiconductores. Desde Mario Draghi hasta la industria, pasando por un conjunto relevante de estados miembros y un grupo de parlamentarios europeos han demandado ya se supla esta carencia. La Comisión Europea, que en un primer momento parecía reacia a reconocer los fracasos de la Chips Act y definía una línea continuista en este ámbito, se presenta ahora dispuesta a rectificar. La vicepresidenta Vikkunen ha liderado este giro de timón declarando que estar planeando "los próximos pasos hacia una Ley de Chips que no está alcanzando los objetivos fijados" (43).

La Brújula de la Competitividad, en definitiva, es un punto de partida de actuaciones que no tiene apenas sorpresas tras el informe Draghi. También de modo implícito ataca las debilidades de la gobernanza digital europea. Sobria en el aspecto regulatorio, excepto en el caso de propuestas largamente pendientes o regulaciones destinadas a promover la inversión, y pretensiones de captar un mayor ámbito decisorio desde Bruselas. No obstante, la Brújula tiene por delante un camino sinuoso para el cumplimiento de sus planes, que la propia Comisión parece dispuesta a rectificar ante la demanda de las partes interesadas, y que habrá de esperarse a ver el desarrollo de su ejecución.

4.5. CONCLUSIONES: LA ÚLTIMA OPORTUNIDAD PARA LA AUTONOMÍA DIGITAL EUROPEA

La autonomía estratégica digital de la Unión Europea se encuentra en una encrucijada crítica. A pesar de los esfuerzos realizados en los últimos años, la UE sigue dependiendo en gran medida de tecnologías extranjeras, lo que la hace vulnerable a las presiones geopolíticas y a las interrupciones de la cadena de suministro. El declive tecnológico ha sido parejo a la disminución de su peso económico. La creciente rivalidad entre Estados Unidos y China ha puesto aún más de manifiesto las debilidades de Europa, carente de actores tecnológicos capaces de rivalizar con las grandes tecnológicas localizadas en las grandes potencias. En particular, la dependencia de la UE respecto de EE. UU. le ha obligado a una alineación geopolítica tecnológica sin crítica con el gigante del nuevo continente. Estamos en un nuevo entorno donde China y EE. UU. están modificando sus visiones de la gobernanza digital nacionales y ello tendrá impacto global. Más promoción de su industria privada en el país del dragón y más proteccionismo en el Nuevo Continente, frente a lo que la UE habrá de renunciar parcialmente a su imperialismo regulatorio y promover más su ecosistema para poder rivalizar con los otros gigantes económicos.

La UE se enfrenta, por tanto, a una oportunidad única para redefinir su papel en el escenario digital mundial. El nuevo ciclo político europeo, con la segunda Comisión Von der Leyen al mando, se presenta como la última oportunidad para revertir la situación de dependencia y construir una Europa digitalmente soberana. El retorno de Donald Trump a la presidencia de EE. UU. presenta un desafío con el renacer de las divergencias de todo tipo incluyendo en la visión tecnológica, pero también puede potenciar el papel de la Unión como facilitador de la ruptura de las tendencias bipolares. Para ello, es crucial que la UE adopte un enfoque holístico que aborde las deficiencias en inversión, innovación, cooperación internacional y gobernanza digital. Los informes elaborados por Enrico Letta y Mario Draghi han facilitado un guion para que las instituciones europeas desarrollen las políticas públicas adecuadas en la esfera digital.

La inversión en I+D+i es fundamental para cerrar la brecha tecnológica con EE. UU. y China. Apoyada en las fortalezas del mercado único, la UE debe priorizar la investigación y el desarrollo en tecnologías digitales clave, como la inteligencia artificial, la computación cuántica y los semiconductores. Europa necesita definir proyectos en estos ámbitos que prioricen los intereses europeos sobre los de los estados miembro y con objetivos concretos, que se apoyen en un entorno favorable para la innovación, que fomente la colaboración entre el sector público y el privado y que atraiga inversión extranjera. A ello pueden contribuir la creación de instrumentos de deuda común —un fondo europeo de soberanía tecnológica— o facilitar los flujos de inversión privada entre los estados miembros —completar mercado único de capitales—. Son reformas estructurales más allá de la tecnología que requerirán grandes dosis de negociación interna, pero que son perentorias.

El desarrollo de una industria digital europea fuerte es esencial para la autonomía estratégica. La UE debe apoyar el crecimiento de las empresas digitales europeas, especialmente las pymes y las *startups*. Es necesario fomentar la creación de clústeres de innovación digital en Europa y promover la adopción de tecnologías digitales por parte de las empresas europeas. Para ello es necesario que Europa disponga de un mercado único de infraestructuras de red y datos que faciliten conexiones de muy alta velocidad, que supere las carencias estructurales actuales que limitan la financiación de sus necesidades. Sin campeones europeos en las infraestructuras digitales la UE no podrá reducir las dependencias en las cadenas de suministro de tecnologías clave y fomentar su producción en Europa.

La cooperación internacional es central también para el éxito de la estrategia digital europea, apoyándose en la misma para impulsar una

vuelta al multilateralismo que permita diversificar las cadenas de suministro. La UE debe fortalecer las alianzas con otros países y regiones que comparten sus valores e intereses en materia digital, apoyada en una diplomacia digital sobre un nuevo modelo interno de gobernanza. La Estrategia Internacional digital de la Unión es un paso en la dirección adecuada. La UE debe agilizar y simplificar la toma de decisiones en materia digital y reforzar la coordinación entre las instituciones europeas, que faciliten una participación activa en foros internacionales y definir conjuntamente con sus aliados proyectos transnacionales que contribuyan al interés común europeo.

El camino hacia la autonomía digital estratégica no será fácil, pero es un camino que la UE debe recorrer si quiere asegurar su futuro en un mundo cada vez más digitalizado. La segunda Comisión Von der Leyen tiene la responsabilidad de liderar este proceso y de construir una Europa digitalmente soberana, innovadora y competitiva. En este sentido, es esperanzador la rápida definición de la Brújula de la Competitividad, toda una hoja de ruta para la puesta en marcha de las reformas propuestas por Mario Draghi que ya ha empezado a materializarse con planes y estrategias detalladas en tecnologías cuánticas e inteligencia artificial. El tiempo apremia y la UE no puede permitirse el lujo de perder esta última oportunidad.

4.6. REFERENCIAS BIBLIOGRÁFICAS

1. Consejo de la Unión Europea. Council conclusions on implementing the EU Global Strategy in the area of Security and Defence [Internet]. 2016 nov. Disponible en: https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf
2. China Power. Will the Dual Circulation Strategy Enable China to Compete in a Post-Pandemic World? [Internet]. 2021 dic, actualizado en 2023 nov. Disponible en: https://chinapower.csis.org/china-covid-dual-circulation-economic-strategy/
3. McKinsey. Reinventing the European economy from within [Internet]. 2023 nov. Disponible en: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/reinventing-the-european-economy-from-within
4. Comisión Europea. Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States [Internet]. 2023 oct. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302113
5. Draghi M. The Draghi report: A competitiveness strategy for Europe (Part A) [Internet]. 2024 sep. Disponible en: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
6. Draghi M. The Draghi report: In-depth analysis and recommendations (Part B) [Internet]. 2024 sep. Disponible en: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
7. Australian Strategic Policy Institute. ASPI's two-decade Critical Technology Tracker [Internet]. 2024 ago. Disponible en: https://www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker
8. Analysys Mason. The State of Digital Communications 2025 [Internet]. 2025 feb. Disponible en: https://connecteurope.org/insights/reports/state-digital-communications-2025
9. Banco Mundial. Disponible en: https://datos.bancomundial.org/indicador/NY.GDP.MKTP.KD.ZG

10. Consejo Europeo. Reunión del Consejo Europeo (29 y 30 de junio de 2023) – Conclusiones [Internet]. 2023 jun. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7-2023-INIT/es/pdf

11. Letta E. Much more than market [Internet]. 2024 abr. Disponible en: https://institutdelors.eu/en/publications/much-more-than-a-market/

12. Jorge R. El papel de España para una Europa más competitiva. Expansión, marzo 2025 [Internet]. Disponible en: https://www.expansion.com/opinion/2025/03/11/67d02cf1e5f-dea04348b4575.html

13. Comisión Europea. Commission presents new initiatives for digital infrastructures of tomorrow [Internet]. 2024 feb. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_941

14. Carnegie Endowment for International Peace. Securing Europe's Subsea Data Cables [Internet]. 2024 dic. Disponible en: https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables

15. Consejo de la Unión Europea. Conclusions on the White Paper "How to master Europe's digital infrastructure needs?" [Internet]. 2024 dic. Disponible en: https://data.consilium.europa.eu/doc/document/ST-16644-2024-INIT/en/pdf

16. Parlamento Europeo. Benefits of EU strategic investment in high-tech digital innovation [Internet]. 2025 feb. Disponible en: https://epthinktank.eu/2025/02/12/benefits-of-eu-strategic-investment-in-high-tech-digital-innovation/

17. Semiconductor Industry Association. Disponible en: https://www.semiconductors.org/about/become-a-member/

18. Observatorio legislativo del Parlamento Europeo. European technological sovereignty and digital infrastructure [Internet]. [citado febrero de 2025]. Disponible en: https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007(INI)

19. Hidalgo M. La Brújula de la Competitividad: Europa en la encrucijada [Internet]. Cinco días. 2025 feb. Disponible en: https://cincodias.elpais.com/economia/2025-02-03/la-brujula-de-la-competitividad-europa-en-la-encrucijada.html

20. Parlamento Europeo. Deepening the single market in the light of the Letta and Draghi reports [Internet]. 2024 oct. Disponible en: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762469

21. Comisión Europea. 2030 Digital Compass: the European way for the Digital Decade [Internet]. 2021 mar. Disponible en: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

22. Comisión Europea. 2023 Report on the state of the Digital Decade [Internet]. 2023 sep. Disponible en: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

23. Parlamento Europeo. Strategic Technologies for Europe Platform: provisional agreement to boost investments in critical technologies [Internet]. 2024 feb. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2024/02/07/strategic-technologies-for-europe-platform-provisional-agreement-to-boost-investments-in-critical-technologies/

24. American Heritage. Mandate for Leadership. The Conservative Promise [Internet]. 2023. Disponible en: https://www.project2025.org/policy/

25. La Casa Blanca. Removing barriers to american leadership in artificial intelligence [Internet]. 2025 ene. Disponible en: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

26. La Casa Blanca. Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties [Internet]. 2025 feb. Disponible en https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/

27. Reuters. Chinese state-linked accounts hyped DeepSeek AI launch ahead of US stock rout, Graphika says [Internet]. 2025 feb. Disponible en: https://www.reuters.com/technology/artificial-intelligence/chinese-state-linked-accounts-hyped-deepseek-ai-launch-ahead-us-stock-rout-2025-01-31/

28. College Towns. Where Did the DeepSeek Team Go to University? Not in the US. 2025 feb. Disponible en: https://collegetowns.substack.com/p/where-did-the-deepseek-team-study

29. The Select Committee on the CCP. Moolenaar, Krishnamoorthi Call For Tightening Export Controls on Chips Critical to China's AI Platform DeepSeek and Other Measures to Address its Risks to Americans' Data and Security [Internet]. 2025 ene. Disponible en: https://selectcommitteeontheccp.house.gov/media/press-releases/moolenaar-krishnamoorthi-call-tightening-export-controls-chips-critical-chinas

30. South China Morning Post. Falling behind is 'biggest security risk' in AI, Chinese political adviser says [Internet]. 2025 mar. Disponible en: https://www.scmp.com/news/china/politics/article/3300873/falling-behind-biggest-security-risk-ai-chinese-political-adviser-says

31. Reuters. Xi's new frontline corporate guard showcases his priorities, control [Internet]. 2025 feb. Disponible en: https://www.reuters.com/world/china/xis-new-frontline-corporate-guard-showcases-his-priorities-control-2025-02-18/

32. Comisión Europea. An International Digital Strategy for the European Union [Internet]. 2025 jun. Disponible en: https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu

33. Arnal J. AI at Risk in the EU: It's Not Regulation, It's Implementation [Internet]. Cambridge University Press. 2025 mar. Disponible en: https://doi.org/10.1017/err.2025.19

34. Strand Consult. What US court ruling on net neutrality means for the rest of the world [Internet]. 2025 ene. Disponible en: https://strandconsult.dk/what-us-court-ruling-on-net-neutrality-means-for-the-rest-of-the-world/

35. Largest Companies by Marketcap. Disponible en: https://companiesmarketcap.com

36. Bradford A. Digital Empires: The Global Battle to Regulate Technology. Oxford University Press; 2023 sep.

37. Comisión Europea. EU digital diplomacy: Council agrees a more concerted European approach to the challenges posed by new digital technologies [Internet]. 2022 jul. Disponible en: https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/

38. Comisión Europea. Political Guidelines 2024-2029 [Internet]. 2024 jul. Disponible en: https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

39. Comisión Europea. European Commission presents its compass to boost Europe's competitiveness in the next five years [Internet]. 2025 ene. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ac_25_385

40. Comisión Europea. Commission sets course for Europe's AI leadership with an ambitious AI Continent Action Plan [Internet]. 2025 abr. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1013

41. Euractiv. US AI dominance: Can Europe create its own Stargate? [Internet]. 2025 ene. Disponible en: https://www.euractiv.de/section/innovation/news/ki-dominanz-der-usa-kann-europa-sein-eigenes-stargate-erschaffen/

42. Comisión Europea. Commission launches strategy to make Europe Quantum leader by 2030 [Internet]. 2025 jul. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1682

43. Reuters. EU's Virkkunen says Commission plans new semiconductor support programme [Internet]. 2025 mar. Disponible en: https://www.reuters.com/technology/eus-virkkunen-says-commission-plans-new-semiconductor-support-programme-2025-03-27/

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

5

El Ciberespacio como nuevo escenario de conflictos. Una visión en el marco de la defensa europea

Fernando Davara Rodríguez

5.1. INTRODUCCIÓN

El panorama geopolítico actual, en permanente evolución, marcado por el retorno de la guerra al Viejo Continente, los conflictos en el Próximo Oriente, el cambio en las relaciones transatlánticas, la multilateralidad y la incertidumbre global, ha vuelto a traer al centro del debate europeo una cuestión cuya importancia no se había considerado como primordial en unos años de estabilidad, paz y crecimiento; la necesidad de hacer frente a los desafíos geoestratégicos que conlleva la defensa de Europa que ha pasado de ser una aspiración a una exigencia estratégica.

Para responder a esta demanda, la Unión Europea y sus estados miembros están rediseñando sus políticas de seguridad y defensa, a las que se otorga la máxima prioridad, incrementando la inversión y gasto en defensa, para disponer de unas capacidades que proporcionen un cierto grado de autonomía estratégica, y redoblando esfuerzos para avanzar hacia una Unión más armonizada al definir las políticas comunes de seguridad y defensa para el nuevo enfoque estratégico.

A tal efecto, la Unión Europea se ha dotado de un amplio marco regulatorio y normativo, completado por un conjunto de instrumentos para su aplicación, y ha adoptado su propia estrategia de seguridad, en la que se incluye de forma específica la del ciberespacio que representa un nuevo escenario de conflictos donde actúan múltiples actores en un dominio virtual y real sin fronteras y fuera del alcance de la soberanía territorial, con unas características que condicionan las estrategias y políticas necesarias no solo para gestionar este espacio sino también, de forma prioritaria, garantizar la ciberseguridad y ciberdefensa conjuntas.

En este sentido, este capítulo está dedicado a exponer como la Unión Europea está afrentando los desafíos inherentes al ciberespacio, en particular en lo que respecta a la ciberdefensa, y a reflexionar sobre los retos que aparecen en el escenario geopolítico actual que dificultan la implantación de una verdadera política de ciberdefensa europea.

Para ello, comenzando por la descripción de los conceptos más directamente relacionados y después de sintetizar las razones por las que el ciberespacio se ha convertido en el quinto escenario de conflictos, que se añade a los anteriores de tierra, mar, aire y espacio exterior, se detallan los aspectos principales de la Estrategia de Ciberseguridad de la Unión Europea relacionados con la ciberdefensa y se lleva a cabo una amplia exposición de la arquitectura europea de ciberseguridad para, entrando ya en el marco de la ciberdefensa, analizar los enfoques de la defensa de Europa que sirven de base a la Política europea de ciberdefensa, analizando su evolución hacia la época actual de incertidumbre global, para concluir con una serie de reflexiones sobre la necesidad de conseguir que sea una política conjunta, segura y resiliente.

5.2. CIBERESPACIO, CIBERSEGURIDAD Y CIBERDEFENSA

El concepto de ciberespacio, contracción de cibernética y espacio, surgió en la década de los 80 cuando el escritor norteamericano William Gibson lo utilizó en su novela de ciencia ficción "Neuromante[1]" para describir un espacio tridimensional generado electrónicamente como "una alucinación colectiva experimentada diariamente por miles de millones de humanos, de todas las naciones, que se encuentran, conversan e intercambian información" (1).

Es decir, un universo paralelo, centrado en la visión humana de este nuevo entorno, con el apoyo de una red virtual de ordenadores

1. William Gibson lo introdujo en 1982 su novela "Burning Chrome" pero se popularizó a partir de su inclusión en 1984 en otra de sus novelas de ciencia ficción titulada "Neuromante".

donde se almacenan grandes cantidades de información que podría utilizarse para adquirir poder con un inmenso potencial de desarrollo de capacidades, así como una extraordinaria complejidad, peculiaridades que caracterizan el ciberespacio de hoy.

Desde entonces, a pesar de que esta ficción no se ha materializado en el sentido en que fue concebida, el vocablo se ha extendido gracias al espectacular desarrollo de las tecnologías de la información y la comunicación, y a su contribución a la formación de una nueva sociedad basada en ellas (2).

Su expansión y universalidad; su rapidez, dinamismo y gran capacidad de acción y crecimiento; su asimetría, caracterizada por la gran facilidad para adquirir los recursos y conocimientos necesarios para actuar en él; la poca exposición y relativa impunidad; el anonimato, al poder llevar a cabo actividades sin que se conozca la identidad del autor, así como su bajo coste financiero, han dado origen a la aparición de múltiples actores con capacidad de actuar en todo tipo de conflictos, razón por la cual se puede considerar al ciberespacio como una nueva realidad geopolítica y estratégica.

Esta afirmación puede parecer una paradoja, pues la geopolítica, por razón de su prefijo (geo), implica poder ligado al territorio, y el ciberespacio no es una realidad geográfica en sentido estricto. Sin embargo, dado que es un espacio real y virtual a la vez, el ciberespacio puede considerarse como un territorio sin Estados, fronteras ni elementos geográficos diferenciadores o delimitadores, en el que existe libre circulación de información, el cual depende tanto de sus componentes físicos y lógicos, interconectados, como de su capa semántica y cognitiva, de elementos intangibles (principalmente datos, información e interacciones sociales) y de los usuarios humanos que interactúan en él y constituyen la base de su dinámica al ser el único espacio creado por ellos sin cuya presencia no podría existir (2).

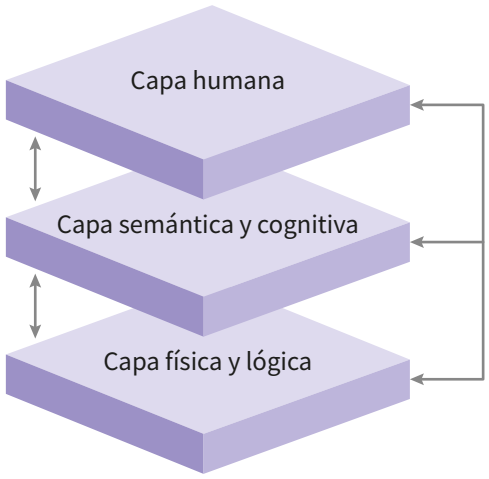


Figura 5.1.
Estructura en capas del ciberespacio.
Elaboración propia.

En consecuencia, es posible afirmar que, con independencia de si se considera o no el ciberespacio como un escenario geopolítico, si existe una geopolítica del ciberespacio, íntimamente ligada a la geopolítica internacional. Este nuevo dominio, que los Estados tratan de utilizar para obtener ventajas estratégicas y desarrollar sus políticas, no surge para reemplazar o minimizar la importancia de los espacios geográficos tradicionales, ni como un entorno aparte, sino como una nueva dimensión para coexistir con ellos presentando nuevos desafíos y haciendo mucho más complejos los equilibrios de poder y las relaciones internacionales (2).

Basado en las tecnologías digitales se ha ido construyendo un entorno social dotado de capacidades, reglas, valores y cultura propias, así como con limitaciones y vulnerabilidades

que no son desconocidas para individuos y organizaciones criminales, terroristas y algunos Estados que han percibido que es un territorio extremadamente útil para alcanzar sus objetivos, para atacar a las potenciales víctimas, destruyendo su información o infraestructura o para obtener informaciones de otros o difundir las suyas propias.

Ante esta evidencia, teniendo en cuenta el volumen cada vez mayor de las amenazas cibernéticas, su sofisticación y gravedad, es preciso afrontar los desafíos que surgen en el ciberespacio, en un escenario global de tensiones e incertidumbres geopolíticas, ampliando el ámbito de la seguridad a este nuevo espacio de conflicto y confrontación, incluyendo en él la ciberseguridad y la ciberdefensa.

Ambos términos se utilizan en numerosas ocasiones de forma similar, e incluso indistintamente, sin establecer una clara definición y diferenciación entre ellos, generando ambigüedad, tanto en lo que respecta al alcance de ambos vocablos como a los desafíos que conllevan, quienes son sus actores y cuáles son los riesgos asociados, razón por la que sin un conocimiento profundo de cuál es su dominio difícilmente podrán proponerse soluciones e implementar medidas de protección y reacción en sus respectivos entornos.

Los dos términos hacen referencia a la seguridad en el ciberespacio, pero con diferentes objetivos, actores y actividades. En principio, en un contexto operativo, aparece el concepto de seguridad en Internet que consiste en la "preservación de la confidencialidad, integridad y disponibilidad de la información a través de Internet" (3) de forma que, por extensión a todo el ciberespacio, que no es únicamente Internet, la ciberseguridad se refiere también a la tecnología, las aplicaciones y servicios que soportan o utilizan la información, así como a las capacidades para proteger o defender el uso del ciberespacio de los ataques cibernéticos.

En este caso puede entenderse que ambos términos son similares con la única diferencia del sector o ámbito que utiliza y protege la información. Sin embargo, en un contexto estratégico, la ciberseguridad abarca no solamente a la información sino también a la "protección de las personas, la sociedad, las organizaciones y las naciones frente a los riesgos cibernéticos" (3) lo que incluye la ciberresiliencia y la ciberdefensa, responsable esta de la protección y supervivencia de los activos que garantizan la Defensa de los Estados o de las organizaciones plurinacionales, como la Unión Europea.

5.3. EL CIBERESPACIO COMO NUEVO ESCENARIO DE CONFLICTOS

Entre los escenarios donde se desarrollan los conflictos actuales, y con toda seguridad los del futuro, a los tradicionales de tierra, mar, aire y espacio exterior se ha unido el ciberespacio, adquiriendo una importancia cada vez mayor debido al auge en el desarrollo, aplicación y utilización de las tecnologías digitales disruptivas que tienen un significativo efecto en alterar o cambiar drásticamente la forma de funcionar y operar prescindiendo de prácticas anteriores.

Su utilización se ha convertido en una prioridad frente a otros espacios para que los actores estatales y no estatales lleven a cabo operaciones como ciberataques o generación de inteligencia y ciberespionaje, constituyendo un multiplicador de fuerza que aumenta significativamente la efectividad de las operaciones militares. Pero también, constituye el entorno ideal para realizar otras muchas actividades como la propaganda y desinformación, la guerra cognitiva o las operaciones psicológicas y de influencia (4).

Dada su importancia al haber invadido todos los ámbitos sociales, públicos y privados, afectando consecuentemente a las actividades propias de los conflictos, cuya eficacia depende en gran parte de la capacidad de acceso y uso del ciberespacio, en lugar de considerarlo como

un dominio más, es coherente estimar que es uno transversal que complementa e influye en los otros cuatro (tierra, mar, aire y espacio exterior) (4); al representarlos por medio de un esquema de múltiples capas se evidencia que el ciberespacio constituye un escenario transversal global de conflictos y por ello presenta desafíos también globales.

En definitiva, el ciberespacio se ha convertido en un nuevo escenario de conflictos con implicaciones geopolíticas que no pueden separarse de las clásicas de los espacios geográficos tradicionales presentando nuevos desafíos a enfrentar mediante un enfoque multiescalar (2).

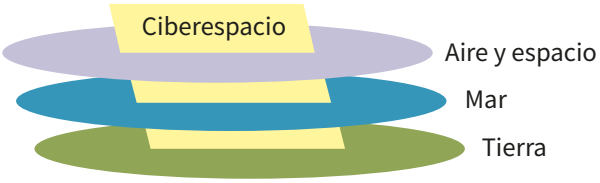


Figura 5.2.
El ciberespacio como espacio transversal de conflictos. Elaboración propia, adaptada de (5).

5.4. ESTRATEGIAS DE CIBERSEGURIDAD EN LA UNIÓN EUROPEA

Hacer frente a los desafíos que presenta el uso seguro del ciberespacio no es solamente una cuestión tecnológica o de seguridad, sino que alcanza el nivel más alto de la estrategia global de las organizaciones, incluyendo a los gobiernos y las organizaciones internacionales.

Para dar respuesta a esta exigencia, en los últimos años muchos Estados y organizaciones plurinacionales, como la Unión Europea, están estableciendo políticas de ciberseguridad. Asimismo, un número no menos importante de ellos han implantado estrategias al más alto nivel de su estructura jerárquica proporcionando el marco adecuado para la dirección y gestión de la seguridad en el ciberespacio fomentando asimismo la cooperación nacional e internacional en la materia.

La práctica habitual es diseñar estos marcos mediante un esquema conocido normalmente como Estrategia Nacional de Ciberseguridad o simplemente Estrategia de Ciberseguridad, en el caso de las organizaciones internacionales, donde se combinan políticas, órganos y procedimientos para garantizar la dirección y gestión de la seguridad en el ciberespacio.

A esta práctica se sumó la Unión Europea cuando, con objeto de hacer frente de forma inequívoca a los desafíos que representan las crecientes amenazas a la seguridad en el ciberespacio, el 7 de febrero de 2013 la Comisión Europea, junto con el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, publicaron su propia estrategia bajo el título de “Estrategia de ciberseguridad de la Unión Europa; un ciberespacio abierto, protegido y seguro” (6).

En la comunicación que la recoge, como ya anticipa su título, se proyecta mantener un ciberespacio abierto, seguro y protegido por medio de la aplicación de un conjunto de medidas enmarcadas en cinco prioridades sintetizadas en:

- Lograr resiliencia cibernética.
- Reducir significativamente los delitos cibernéticos.
- Desarrollar una política y unos medios de ciberdefensa en conjunción con la Política Común de Seguridad y Defensa (PCSD), anteriormente Política Europea de Seguridad y Defensa (PESD).
- Desarrollar recursos industriales y tecnológicos en ciberseguridad.
- Establecer una política internacional coherente de la Unión Europea en materia cibernética y promover los valores fundamentales de la UE.

La estrategia englobaba múltiples aspectos del ciberespacio en materias tan diferentes como los recursos industriales y tecnológicos, la justicia, la política exterior y de defensa, etc., expresándose en ella unos principios fundamentales que deberían servir de guía para la política internacional de la Unión en materia de ciberseguridad y de aplicación en otros dominios.

Posteriormente, el 16 diciembre de 2020, en respuesta a la crisis provocada por la pandemia declarada por la Organización Mundial de la Salud por la expansión a escala mundial del coronavirus y como consecuencia el considerable aumento del teletrabajo, la Comisión Europea y el Alto Representante para Asuntos Exteriores y Política de Seguridad presentaron públicamente la nueva Estrategia de Ciberseguridad de la Unión Europea (La Estrategia de Ciberseguridad de la UE para la Década Digital) (7) diseñada con la finalidad de reforzar la resiliencia conjunta frente a las ciberamenazas así como para garantizar que ciudadanos y empresas se beneficien de servicios y herramientas digitales seguros y fiables.

Considerada un componente clave de los diferentes planes de respuesta a la crisis provocada por la COVID-19, como el Plan de Recuperación Next Generation EU, así como la Estrategia Global para la Política Exterior y de Seguridad de la UE[2], la nueva Estrategia de Ciberseguridad tiene por objeto promover un ciberespacio abierto y global no solo para garantizar la seguridad, sino también para proteger los valores europeos y los derechos fundamentales de todos.

Para alcanzar tales objetivos, en esta nueva versión, actualización de la publicada en 2013, se incluyen propuestas concretas para el despliegue de tres instrumentos, normativos, de inversión y de política, que aborden todas las áreas de acción de la Unión. Entre ellas destacan algunas que pueden calificarse de novedosas como la revisión del marco regulatorio vigente en Europa, el fortalecimiento de las capacidades de prevención, disuasión y respuesta y la voluntad de asegurar la próxima generación de redes (5G y siguientes).

Basándose en los avances logrados desde la publicación de la edición anterior, en esta se abordan las futuras áreas de actuación de la Unión Europea en materia de ciberseguridad basándose en tres pilares fundamentales:

- Resiliencia, soberanía tecnológica y liderazgo.
- Desarrollo de la capacidad operativa para prevenir, disuadir y responder.
- Cooperación para promover un ciberespacio global y abierto (7).

El segundo de ellos recoge algunas propuestas concretas relacionadas con la ciberdefensa como la creación de una Unidad Cibernética Conjunta que refuerce el marco europeo de gestión de crisis de ciberseguridad, o la revisión del Marco de política de defensa cibernética y el desarrollo de la "Visión" y estrategia militar sobre el ciberespacio para las misiones y operaciones militares de la PCSD (7).

Otras actuaciones contempladas en esta área se refieren a apoyar las sinergias entre las industrias civil, de defensa y espacial y fomentar y facilitar el establecimiento de un grupo de trabajo de ciberinteligencia de los Estados miembros que resida dentro del INTCEN[3] de la Unión.

2. Estrategia Global para la Política Exterior y de Seguridad de la UE (junio 2016).

3. INTCEN, Centro de Inteligencia y Situación de la Unión Europea (EU Intelligence and Situation Centre, EU INTCEN); uno de los órganos de Inteligencia de la Unión que forma parte desde el año 2011 del Servicio Europeo de Acción Exterior (SEAE), dependiendo del vicepresidente de la Comisión, el Alto Representante para Asuntos Exteriores y Política de Seguridad.

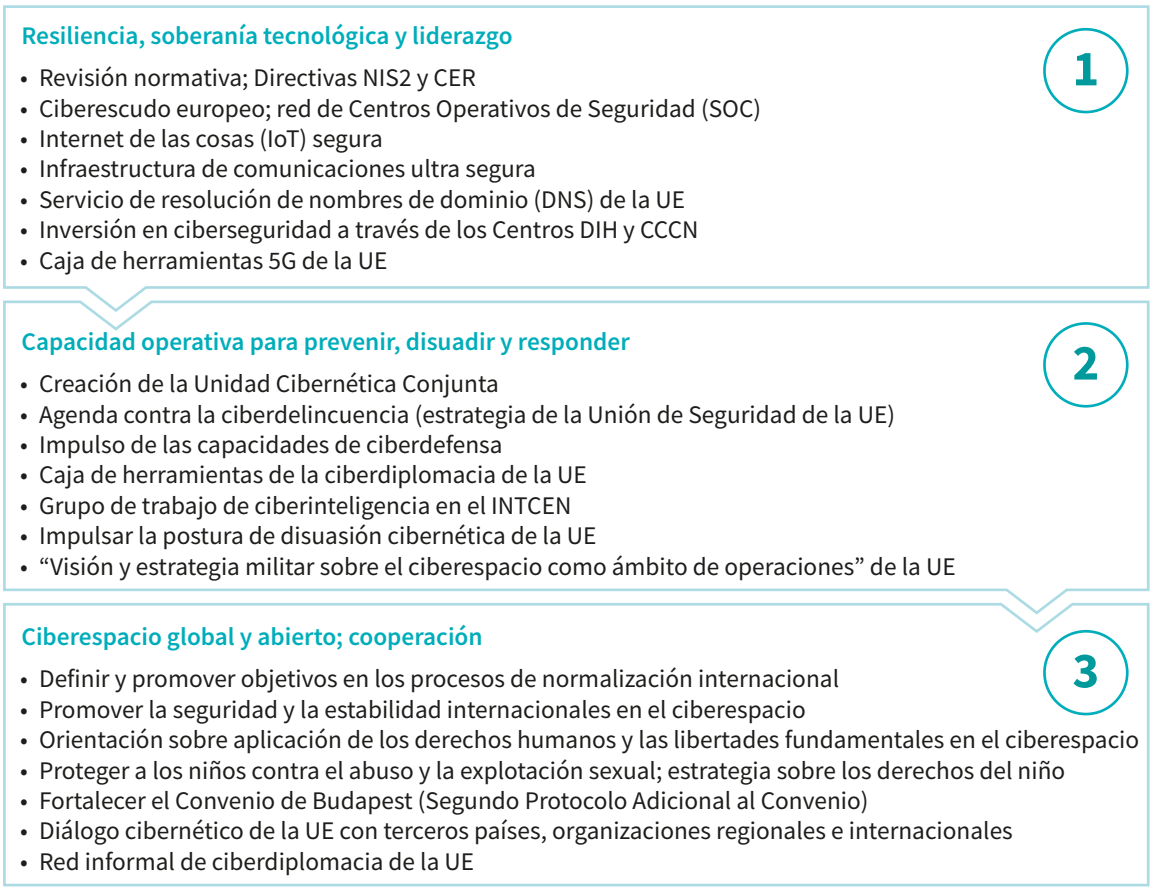


Figura 5.3.
Pilares de la Estrategia de Ciberseguridad de la Unión Europea.
Elaboración propia derivado de (7).

5.5. ARQUITECTURA EUROPEA DE CIBERSEGURIDAD

En el marco de este documento se entiende como arquitectura de ciberseguridad a la estructura estratégica de todos los componentes de la seguridad cibernética de una organización, en este caso plurinacional como es la Unión Europea, así como a sus relaciones, tanto entre ellos como con su entorno, y a los principios que guían su concepción y evolución.

Fundamentada en una fuerte cooperación entre las instituciones comunitarias, los Estados miembros y el sector privado, la arquitectura de ciberseguridad de la Unión Europea se estructura en torno a un complejo ecosistema que agrupa estrategias, políticas, organismos y entidades, regulación y normativa, capacidades y procedimientos, que configuran un conjunto cuyo principal objetivo es garantizar un elevado nivel de seguridad cibernética en toda la Unión.

Entre los componentes que lo integran destacan los que se exponen en los siguientes apartados:

5.5.1. Marco normativo y legal

Desde comienzos del siglo XXI la Unión estuvo adoptando todo tipo de iniciativas para reforzar la ciberseguridad y proteger datos, información y comunicaciones en múltiples sectores dependientes cada vez más de las tecnologías digitales.

Pero en el ciberescenario geopolítico actual surgen múltiples actores, entre los que se encuentran los Estados o gobiernos, el sector privado, organizaciones de todo tipo, como las tecnológicas con fuerte presencia, o los criminales que operan en la red oscura o *darkweb*, grupos terroristas, *hackers* y ciberactivistas, y también los usuarios que conforman la denominada sociedad civil que de forma individual o colectiva actúa para compartir información y defender sus intereses (2).

Tal complejidad demanda un marco regulatorio más amplio cuya consecuencia ha sido la elaboración y adopción de un amplio paquete legislativo y normativo sobre seguridad cibernética que, junto a las diversas herramientas destinadas a aplicar las disposiciones legislativas, conforman la arquitectura de ciberseguridad europea.

Este conjunto está constituido, entre otros, por la Estrategia Europea de Ciberseguridad (2020), expuesta con anterioridad, y los documentos que se exponen a continuación en este apartado.

Reglamento General de Protección de Datos (RGPD) de la Unión Europea

El Reglamento General de Protección de Datos (RGPD), aprobado por el Parlamento europeo en abril de 2016, entrando en vigor en mayo de 2018, se publicó con el objetivo de reforzar la protección de los datos personales de los ciudadanos de la Unión Europea, constituyendo en su época uno de los instrumentos legislativos más importantes de la Unión cuya característica principal es la relativa a su rango y alcance.

Hasta su promulgación la protección de datos en la Unión Europea se regía por una Directiva, la 95/46/CE, que ahora se sustituye por medio de un Reglamento, diferencia que pudiera parecer poco significativa, pero señala de forma clara el dominio de aplicación del RGPD.

En la Unión Europea las directivas no son legalmente vinculantes, pues se consideran como recomendaciones que cada Estado miembro puede interpretar, sin obligación de aplicarlas; sin embargo, un reglamento es similar a una ley, cuyas normas son de obligado cumplimiento.

Esto significa que el GDPR constituye un marco jurídico unificado directamente aplicable en el conjunto de los Estados miembros a partir del 25 de mayo de 2018, fecha que se fijó para su ejecución, sin necesidad de transposiciones, de forma que los tratamientos que existan posteriormente deberán ser conformes con lo dispuesto en el Reglamento (8).

En el ámbito de la ciberseguridad sus principales tareas y obligaciones hacen referencia a la protección de los datos personales, privacidad, por diseño y por defecto, gestión de brechas de seguridad, obligación de notificar las violaciones de datos, responsabilidad y rendición de cuentas ante accesos no autorizados, fugas o pérdidas, seguridad en la transferencia de datos fuera de la Unión Europea y evaluación y mitigación de los riesgos de ciberseguridad.

Directivas sobre redes y sistemas de información (Directivas NIS1 y NIS2)

Continuando con las medidas encaminadas a garantizar la ciberseguridad comunitaria, y también la de alcance global, después de la presentación de la primera de las Estrategias de Ciberseguridad de la Unión Europea (2013) y la aprobación en 2016 del reglamento GDPR, el 6 de julio de ese mismo año se completó el paquete de medidas con la adopción de una iniciativa conocida como Directiva NIS titulada "Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión" (9).

Por medio de esta Directiva, considerada en su momento como la primera legislación sobre

ciberseguridad que afecta a todos los Estados miembros, que deberán cumplir una serie de requisitos mínimos comunes, se trataba de lograr un alto nivel común de seguridad de las redes y sistemas de información dentro de la Unión con el fin de mejorar el funcionamiento del mercado interior.

Teniendo como principal objetivo el mejorar la ciberseguridad de las empresas estaba dirigida a dos figuras de importancia en su aplicación: los operadores de servicios esenciales, como energía, salud, transporte, etc., definidos como una entidad pública o privada que presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, cuya prestación depende de las redes y sistemas de información y donde un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio, y el proveedor de servicios digitales, que es toda persona jurídica que preste un servicio de este tipo, entre los que se incluyen los motores de búsqueda y los servicios en la Nube (8) (9).

A ambos la Directiva exigía que cumplieran con las medidas de ciberseguridad adecuadas para gestionar los riesgos inherentes a la seguridad de las redes y los sistemas de información utilizados para la prestación de sus servicios, garantizando un nivel de seguridad adecuado en relación con el riesgo planteado, e informaran sobre cualquier incidente importante de ciberseguridad que experimentaran.

A su vez, para promover una cooperación operativa eficaz entre la Unión y los Estados miembros, se creaban una serie de instrumentos que incluían, entre otros, un grupo de cooperación[4], para apoyar y facilitar la cooperación estratégica, el intercambio de información y la confianza y seguridad entre ellos, y una red de equipos de respuesta a incidentes de seguridad informática (red de CSIRT), que se tratará en un apartado posterior.

El considerable aumento del número de ciberataques a las empresas e infraestructuras críticas de los Estados miembros, en particular debido al impacto de la pandemia del COVID-19 en el incremento del uso de las tecnologías digitales y al nuevo entorno geopolítico, manifestaron la limitación del alcance de la Directiva NIS, por lo que el Consejo y el Parlamento, con objeto de elevar el nivel básico de resistencia de la ciberseguridad en toda la Unión, decidieron adoptar en diciembre de 2022 su actualización, por medio de una nueva Directiva (10), conocida por su acrónimo como NIS2, derogando la anterior que pasó a denominarse como la NIS1.

Como descendiente de la anterior Directiva, la NIS2 mantiene el objetivo de alcanzar un elevado nivel común de ciberseguridad en toda la Unión, pero introduciendo mejoras significativas ampliando su ámbito de aplicación, introduciendo requisitos más estrictos y reforzando las medidas de ejecución y poniendo un mayor énfasis en la colaboración transfronteriza.

En el primer caso, la ampliación del ámbito de aplicación, la NIS2 abarca una mayor número de sectores añadiendo las entidades que denomina "esenciales" en un número de quince, donde se encuentran, entre otras, el transporte, la banca, la energía, la sanidad, las tecnologías de la información y las infraestructuras digitales, así como otras consideradas como "importantes" cuyo número de seis reúne a los servicios de correo y mensajería, la gestión de residuos, producción, procesamiento y distribución de alimentos, fabricación, producción y distribución de productos químicos, los proveedores digitales y la investigación (10).

En cuanto a la colaboración, la NIS2 pretende mejorar la cooperación transfronteriza y el intercambio de información entre los Estados miembros mediante la creación de un nuevo Grupo de Cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y para fortalecer la confianza y la colaboración, y de una Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLON), que se expondrá posteriormente, con el objetivo de favorecer la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran

4. Integrado por los Estados miembros, la Comisión Europea y la Agencia de la UE para la Ciberseguridad (ENISA).

escala en el ámbito operativo y de garantizar el intercambio regular de información relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión (10).

Como se expuso anteriormente, al ser la NIS2 una Directiva y no un Reglamento, es aplicable directamente en los Estados miembros hasta su transposición al derecho nacional, de forma que las legislaciones de cada uno de ellos deberían modificar las leyes afectadas por la Directiva antes de la fecha límite que establecieron los legisladores europeos, el 17 de octubre de 2024.

Ley de Ciberseguridad de la Unión Europea

En junio de 2019, la Unión Europea adoptó la Ley de Ciberseguridad de la UE (11) cuyo objetivo era fortalecer el mandato de la hasta entonces denominada Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y establecer un marco de certificación de ciberseguridad a nivel de la UE para productos, servicios y procesos de Tecnologías de la información y comunicaciones.

Este marco proporciona un sistema para establecer esquemas europeos de emisión de certificados europeos de ciberseguridad con el fin de mantener la confianza y la seguridad de que los productos, servicios y procesos TIC evaluados conforme a dichos esquemas cumplen con los requisitos de seguridad especificados (11).

Por otra parte, el Reglamento cambió el nombre de ENISA por el de Agencia de la Unión Europea para la ciberseguridad otorgando un mandato permanente a esta organización con mayores responsabilidades, más recursos y nuevas funciones, como se expondrá posteriormente en el apartado dedicado a esta Agencia.

Ley de Resiliencia Operativa Digital (DORA)

La Ley de Resiliencia Operativa Digital (Unión Europea, Reglamento (UE) 2022/2554, 14 de diciembre 2022) o DORA, es un Reglamento de la Unión Europea adoptado en 2022 para fortalecer la resiliencia digital de las entidades financieras y garantizar que puedan resistir, responder y recuperarse no solamente ante ciberataques sino también cualquier tipo de incidente cibernético, como por ejemplo fallos del sistema.

El Reglamento DORA se aplica a todas las instituciones financieras de la UE, incluidos bancos e inversionistas, y a los proveedores de servicios externos que suministran a estas instituciones sistemas y servicios de TIC, como los proveedores de servicios en la nube y los centros de datos.

Su cumplimiento exige a dichas entidades establecer un conjunto de requisitos técnicos que incluyen la gestión de riesgos digitales, así como los que presentan los proveedores externos, la notificación de incidentes, realización de pruebas de resiliencia operativa y el intercambio de información entre ellas.

En su conjunto, DORA es un paquete de medidas legislativas aprobadas para tratar de armonizar las normas relativas a gestión y mitigación de riesgos de las TIC en el sector financiero, cuyo nivel superior lo constituyen dos piezas, la Ley DORA y la Directiva (UE) 2022/2556, adoptada el 14 de diciembre de 2022, por medio de la cual se introducen modificaciones en otras Directivas clave para fortalecer la resiliencia operativa digital del sector financiero en la Unión Europea.

Ley de Ciberresiliencia de la Unión Europea (CRA)

En el marco del primer pilar (resiliencia, soberanía tecnológica y liderazgo) de la Estrategia de Ciberseguridad de la Unión Europea (2020), en octubre de 2024 la Unión adoptó la Ley de Ciberresiliencia (CRA, Cyber Resilience Act, Reglamento (UE) 2024/2847, 23

octubre 2024) como marco legal que describe los requisitos de ciberseguridad para productos *hardware* y *software* con componentes digitales y sus soluciones de procesamiento remoto de datos comercializados en la Unión.

El Reglamento se aplica a los productos "críticos" con elementos digitales, es decir, a un producto con elementos digitales que presente un riesgo de ciberseguridad de acuerdo con los criterios establecidos. Sus obligaciones incluyen la ciberseguridad desde el diseño, gestión de vulnerabilidades y la vigilancia del mercado y afectan a tres operadores: fabricantes, importadores y distribuidores de productos con elementos digitales disponibles en la UE.

La ley entró en vigor el 10 de diciembre de 2024 y sus principales obligaciones se aplicarán a partir del 11 de diciembre de 2027, fecha a partir de la cual los productos con elementos digitales, incluidos *hardware*, *software* y servicios de apoyo, que no cumplan sus requisitos no podrán venderse en la Unión Europea.

Ley de Cibersolidaridad de la Unión Europea (CSA)

Finalmente, a modo de culminación de todo este paquete legislativo, el 19 de diciembre de 2024 se publicó la conocida como Ley de Cibersolidaridad de la Unión Europea (CSA, Cyber Solidarity Act, Reglamento (UE) 2025/38, 19 diciembre 2024) con los objetivos de reforzar la solidaridad y las capacidades en la Unión Europea para conocer la situación, detectar, prepararse y responder a ciberamenazas e incidentes, estableciendo un marco robusto y común en materia de seguridad cibernética.

Tales estos objetivos se alcanzarán mediante la creación de los siguientes instrumentos:

- Despliegue de una red paneuropea de centros cibernéticos nacionales y transfronterizos, denominada "Sistema Europeo de Alerta de Ciberseguridad" a fin de desarrollar y mejorar las capacidades coordinadas de detección y la conciencia situacional común.
- Creación de un "mecanismo de emergencia en materia de ciberseguridad" para ayudar a los Estados miembros y a otros usuarios a prepararse para incidentes de ciberseguridad significativos y a gran escala, responder a ellos, mitigar sus efectos y recuperarse.

  Este mecanismo incluye la creación de una "reserva de ciberseguridad de la Unión Europea" compuesta por servicios de respuesta a incidentes del sector privado disponibles para intervenir a petición de un Estado miembro o de instituciones, organismos y agencias de la Unión, así como de terceros países asociados, en caso de un incidente de ciberseguridad significativo o a gran escala.
- Establecimiento de un "mecanismo europeo de revisión de incidentes de ciberseguridad" para revisar y evaluar incidentes de ciberseguridad significativos o a gran escala (12).

Esta ley completa los vacíos de las regulaciones anteriores pues con ella se trata de conseguir la preparación colectiva, la respuesta rápida y establecer un marco común de capacidades europeas de ciberseguridad para asegurar que las amenazas y ataques cibernéticos no sean solo un problema nacional, sino una responsabilidad de toda la Unión.

5.5.2. Capacidades (actores, soluciones y servicios)

La aplicación de la regulación, normativa e iniciativas para asegurar la ciberseguridad de la Unión Europea, corresponde a un amplio conjunto de instituciones y organismos comunitarios que cooperan en el ámbito de la ciberdefensa, como la Comisión Europea,

el Servicio Europeo de Acción Exterior (SEAE)[5] y la Agencia Europea de Defensa (AED)[6], dependiendo asimismo de unas capacidades concretas caracterizadas por unos actores clave entre los que se incluyen los siguientes:

ENISA, la agencia de ciberseguridad de la Unión Europea

ENISA[7], la agencia de la Unión Europea que se ocupa de la ciberseguridad, es responsable de contribuir a la política cibernética y al desarrollo del sector de la ciberseguridad de la Unión Europea, prestar apoyo y cooperar con los Estados miembros, las instituciones de la Unión Europea, universidades, organismos de investigación y las empresas, aportar soluciones y mejoras para la confiabilidad de los productos, servicios y procesos de TIC con esquemas de certificación de ciberseguridad.

Creada en el año 2004 con el nombre de Agencia Europea de Seguridad de las Redes y de la Información (ENISA) con el objetivo de contribuir al establecimiento de un elevado y efectivo nivel de seguridad de las redes y de la información en la Unión y al desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de los ciudadanos, los consumidores, las empresas y las administraciones públicas (13).

Su mandato se ha ido prorrogando mediante sucesivos Reglamentos (1007/2008, 580/2011 y 526/2013) hasta el año 2019 cuando se consideró necesario revisar su mandato para definir su función en el nuevo ecosistema de la ciberseguridad y garantizar su contribución eficaz a configurar la respuesta de la Unión a los desafíos de ciberseguridad derivados de la transformación radical de las amenazas.

Como respuesta a esta necesidad, en abril de 2019, por medio de la anteriormente mencionada Ley de Ciberseguridad, se estableció que ENISA, con la nueva denominación de Agencia de la Unión Europea para la ciberseguridad, sucediera a ENISA tal como fue creada por el Reglamento del año 2013, desempeñando su cometido con el fin de lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros, a las instituciones, órganos y organismos de la Unión en la mejora de la ciberseguridad (11).

También se señala en el Reglamento que ENISA actuará como punto de referencia de asesoramiento y conocimientos especializados en cuestiones relacionadas con la ciberseguridad para las instituciones, órganos y organismos de la Unión, así como para otras partes interesadas pertinentes de la Unión.

Sus tareas, recogidas en los artículos 5 al 12 del Reglamento, se sintetizan en las siguientes:

- Contribución a la elaboración y aplicación de la política y la legislación de la Unión Europea en el ámbito de la ciberseguridad.
- Creación de capacidades, en particular mediante la asistencia de los Estados miembros y a otras estructuras e instituciones.
- Cooperación operativa a nivel de instituciones de la Unión Europea, Estados miembros y entidades, así como la realización de ejercicios de ciberseguridad.

5. Servicio Europeo de Acción Exterior (SEAE): es el servicio diplomático de la Unión Europea. Su objetivo es desarrollar una política exterior de la Unión de forma coherente y eficaz y aumentar así la influencia de Europa en el mundo. Está dirigido por el Alto representante para Asuntos Exteriores y Política de Seguridad.

6. Agencia Europea de Defensa (AED): apoya a los Estados miembros a mejorar las capacidades de defensa por medio de la cooperación europea; actúa como operador central de las actividades relacionadas con la defensa financiadas por la UE. Está dirigida por Alto representante para Asuntos Exteriores y Política de Seguridad.

7. ENISA (European Union Agency for Cybersecurity): Agencia de la Unión Europea para la ciberseguridad.

- Apoyo y promoción en el desarrollo y la aplicación de la política de la Unión sobre certificación de la ciberseguridad de los productos, servicios y procesos de tecnologías de la información.
- Análisis de tecnologías, recopilación y difusión de información.
- Concienciación pública sobre los riesgos y educación en ciberseguridad.
- Investigación e innovación, en particular asesorando a las instituciones europeas sobre los ámbitos que deben priorizarse y contribuyendo al programa estratégico de investigación e innovación.
- Cooperación internacional con terceros países y organizaciones internacionales con el fin de promover la cooperación internacional en cuestiones de ciberseguridad (11).

La promulgación de esta Ley de Ciberseguridad de la Unión Europea otorgó a ENISA un mandato permanente con más tareas, recursos y también más responsabilidades, en particular al determinar en su artículo 7 que la Agencia se hace cargo de la secretaría de la red de CSIRT, de conformidad con el artículo 12, apartado 2, de la Directiva NIS, y como tal apoyará activamente el intercambio de información y la cooperación entre sus miembros (11).

Equipo de Respuesta a Emergencias Informáticas (CERT-EU, Computer Emergency Response Team)

Establecido de forma provisional en 2011, fue creado oficialmente en 2017 por medio de un Acuerdo (14) entre diversas instituciones europeas sobre la organización y el funcionamiento de un Equipo de respuesta a emergencias informáticas de las instituciones, órganos y agencias de la Unión (CERT-Unión Europea).

Diseñado para garantizar una respuesta coordinada de la Unión a los ciberataques contra sus instituciones, el CERT-Unión Europea es un servicio interinstitucional permanente cuya función principal es la de contribuir a la seguridad de las infraestructuras de las Tecnologías de la Información y las Comunicaciones (TIC) de todas las instituciones, órganos y agencias de la Unión ayudando a prevenir, detectar, mitigar y dar respuesta a los ataques cibernéticos, actuando como una plataforma de coordinación de la respuesta a incidentes de ciberseguridad y del intercambio de información (14).

Para cumplir tal misión se encarga, según lo recogido en el artículo 2 del acuerdo, de recopilar, gestionar, analizar y compartir información sobre posibles amenazas, vulnerabilidades e incluso, incidentes que tienen que ver con las infraestructuras de las TIC no clasificadas, aunque puede prestar asistencia en incidentes en las redes o sistemas informáticos clasificados si así se le solicita (14).

Asimismo coordina la respuesta incidentes de ciberseguridad, a escala institucional e interinstitucional, proporciona y coordina la prestación de asistencia operativa especializada, realizando además evaluaciones técnicas y de monitoreo de ciberamenazas, cooperando e intercambiando información, de conformidad con el principio de "necesidad de compartir", con los CERT nacionales o gubernamentales de los Estados miembros de la Unión Europea, en particular a través de la red de CSIRT a que se refiere el artículo 12 de la Directiva NIS (14).

El CERT se activó por primera vez en enero de 2022, poco antes del inicio de la invasión rusa de Ucrania, para hacer un seguimiento del panorama cibernético global y anticipar si las operaciones cibernéticas se dirigirían contra las instituciones, organismos y agencias de la Unión Europea, organizaciones en Ucrania y otros países de la Unión Europea.

Red de CSIRT[8]/CERT[9]

Un Equipo de respuesta a ciberincidentes (CSIRT) es una organización estructural específica encargada de organizar y pilotar la gestión de ciberincidentes. Se materializa por medio de un reducido grupo de personas de diferentes áreas de la propia organización, y eventualmente externas a ella, con el conocimiento y experiencia suficientes, organizadas según un estilo de geometría variable adaptada a las diferentes situaciones de ciberincidentes que pueden producirse.

El 2016, con el fin de contribuir al desarrollo de la confianza entre los Estados miembros y promover una cooperación operativa rápida y eficaz, la Directiva NIS estableció una red de CSIRT integrada por los CSIRT nacionales y el CERT-EU, con la participación de la Comisión Europea en calidad de observador y ENISA, que además de encargarse de la secretaría presta asistencia activa para la cooperación entre los CSIRT.

Posteriormente, en 2022, la nueva Directiva (NIS2) reforzó su papel asignando entre otras las siguientes tareas:

- Intercambiar información sobre las capacidades de los CSIRT.
- Facilitar el intercambio, la transferencia y la puesta en común de tecnología y medidas, políticas, herramientas, procesos, mejores prácticas y marcos pertinentes entre los CSIRT.
- Intercambiar información relevante sobre incidentes, cuasi accidentes, amenazas cibernéticas, riesgos y vulnerabilidades.
- Intercambiar información sobre publicaciones y recomendaciones en materia de ciberseguridad.
- Garantizar la interoperabilidad en lo que respecta a las especificaciones y protocolos de intercambio de información (10).

En cumplimiento de lo dispuesto en la NIS2 cada Estado miembro debe designar o establecer uno o más CSIRT que deberán cumplir los requisitos establecidos en la propia Directiva y serán responsables de la gestión de incidentes conforme a un proceso bien definido.

Centros ISAC

Los Centros de Intercambio y Análisis de Información (ISAC, Information Sharing & Analysis Centre) son organizaciones sin ánimo de lucro que proporcionan un recurso central para recopilar información sobre ciberamenazas además de permitir el intercambio bidireccional de información sobre incidentes y amenazas entre los sectores público y privado, así como el intercambio de experiencias, conocimientos y análisis.

Diversas legislaciones y normativas europeas como la Directiva NIS y la Ley de Ciberseguridad impulsaron la creación de ISAC sectoriales, europeos y nacionales, como asociaciones público-privadas, sin ánimo de

8. CSIRT, Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Ciberseguridad).

9. Estos dos acrónimos se utilizan habitualmente como sinónimos, aunque existe una diferencia. El acrónimo CERT fue registrado oficialmente en la Oficina de Patentes y Marcas Registradas de EE. UU. por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon por lo que quedó reservado para determinados ámbitos de forma que los CSIRT que quieran usar el término CERT deben solicitar su autorización al SEI.

   En consecuencia, realmente no existen diferencias entre un CERT y un CSIRT excepto en el hecho de la necesidad de autorización para la utilización formal del primer término por parte del mencionado Instituto, como son por ejemplo en España los casos del CCN/CERT o del INCIBE CERT.

lucro, entre partes interesadas expuestas a vulnerabilidades y amenazas en materia de ciberseguridad dentro de la Unión Europea.

Los ISAC, normalmente compuestos por iniciativas privadas, en particular los operadores de servicios esenciales de los sectores de infraestructuras críticas, reúnen, analizan y difunden bidireccionalmente a sus miembros información sobre incidentes y amenazas y proporcionan instrumentos y soluciones para mitigar los riesgos y aumentar la capacidad de recuperación.

Al estar estrechamente vinculados con la Comisión Europea y ENISA, trabajan junto con ambas instituciones para colaborar y desarrollar ISACs, tanto a nivel de la Unión Europea como nacional, y promover nuevos ISAC en sectores que todavía no están cubiertos. Entre ellos se encuentran el Centro Europeo de Intercambio de Información y Análisis sobre Energía (EE-ISAC, European Energy Information Sharing & Analysis Centre), y el Centro de Análisis e Intercambio de Información Espacial de la Unión Europea (EU Space ISAC, EU Space Information Sharing Centre).

5.5.3. Financiación y recursos

La financiación de la ciberseguridad se obtiene a través de diferentes medios destacando entre ellos los que contemplan los Fondos de Recuperación (Next Generation Funds EU) establecidos por la Unión Europea en diciembre de 2020 como un instrumento excepcional de recuperación temporal con el fin de hacer frente a la crisis económica derivada de la COVID-19, que incluyen a la ciberseguridad en diversos programas como el plan de recuperación para Europa, dentro del Programa Europa Digital.

Este Programa (Europa Digital) se estableció en abril de 2021 por medio del Reglamento 2021/694 para la contribución financiera de la Unión al marco plurianual 2021-2027 con varios objetivos generales como apoyar y acelerar la transformación digital de la economía, la industria y la sociedad europeas; hacer llegar sus beneficios a los ciudadanos, las administraciones públicas y las empresas de toda la Unión; y mejorar la competitividad de Europa en la economía digital global, contribuyendo al mismo tiempo a reducir la brecha digital en toda la Unión y a reforzar su autonomía estratégica mediante un apoyo holístico, intersectorial y transfronterizo y una mayor contribución de la Unión (15).

Entre los objetivos específicos se incluye uno denominado ciberseguridad y confianza por medio del cual se trata de:

- Apoyar la creación y adquisición de equipos, herramientas e infraestructuras de datos avanzados de ciberseguridad, junto con los Estados miembros, con el fin de lograr un alto nivel común de ciberseguridad a nivel europeo.
- Apoyar la creación y el mejor uso de los conocimientos, capacidades y habilidades europeas relacionadas con la ciberseguridad, así como el intercambio y la integración de las mejores prácticas.
- Garantizar un amplio despliegue de soluciones de ciberseguridad eficaces y de última generación en toda la economía europea, prestando especial atención a las autoridades públicas y las pymes.
- Reforzar las capacidades de los Estados miembros y del sector privado para ayudarlos a cumplir la Directiva NIS, incluso mediante medidas de apoyo a la adopción de las mejores prácticas en materia de ciberseguridad.
- Mejorar la resiliencia frente a los ciberataques, contribuir a aumentar la concienciación sobre los riesgos y el conocimiento de los procesos de ciberseguridad, apoyar a las organizaciones públicas y privadas para alcanzar niveles básicos de ciberseguridad.
- Mejorar la cooperación entre los ámbitos civil y de defensa en lo que respecta a

proyectos, servicios, competencias y aplicaciones de doble uso en ciberseguridad, de conformidad con el Reglamento por el que se establece el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (15).

En el Reglamento se especifica que las acciones en el marco de este objetivo específico se ejecutarán principalmente a través del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y de la Red de Centros Nacionales de Coordinación, de conformidad con el Reglamento del Centro de Competencia en Ciberseguridad (15).

5.5.4. Cooperación

Centro Europeo de Competencia en Ciberseguridad (ECCC) y Red de Centros Nacionales de Coordinación (NCC)

Por medio del Reglamento (UE) 2021/887 de la Unión Europea se creó el Centro Europeo de Competencia en Ciberseguridad (ECCC, European Cybersecurity Competence Centre) estableciendo a su vez la Red de Centros Nacionales de Coordinación (NCCs, Network of National Coordination Centres), los cuales, trabajando conjuntamente, constituyen el nuevo sistema destinado a apoyar la innovación y la política industrial en materia de ciberseguridad a escala europea para fortalecer las capacidades del sector al permitir el despliegue y la adquisición de soluciones innovadoras, facilitando la colaboración y el intercambio de conocimientos y capacidades entre todas las partes interesadas, en particular las comunidades investigadoras e industriales.

Según se dispone en el Reglamento cada Estado miembro designará un Centro de coordinación nacional los cuales servirán como puntos de contacto nacionales para el ECC, a modo de "guardianes" de la comunidad de ciberseguridad en cada país (16).

Como se indicó anteriormente el Centro y la Red desempeñan un papel clave en el cumplimiento de los objetivos de ciberseguridad del Programa Europa Digital.

Red CyClone

La Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe) fue creada por la Directiva NIS2 (artículo 16) como se expuso anteriormente, con el fin de contribuir a la gestión coordinada de los incidentes y las crisis de ciberseguridad a gran escala en el ámbito operativo y de garantizar el intercambio regular de información relevante entre los Estados miembros y las instituciones, los órganos y los organismos de la Unión.

Integrada por representantes de las autoridades de gestión de crisis de ciberseguridad de los Estados miembros y, en determinados casos también por la Comisión, cuando un incidente de ciberseguridad pueda tener un impacto significativo en los servicios y actividades incluidos en dicha Directiva, promoverá, a través de ENISA, el intercambio seguro de información y facilitará las herramientas necesarias al objeto de respaldar la cooperación entre los Estados miembros (10).

Entre sus principales cometidos destaca el desarrollar una conciencia situacional conjunta de los incidentes y crisis de ciberseguridad a gran escala, evaluar sus consecuencias si se producen, proponiendo posibles medidas para mitigar sus efectos, coordinar su gestión y apoyar a la toma de decisiones a nivel político en relación con tales incidentes y crisis.

Grupo de cooperación NIS

Como se expuso anteriormente, la Directiva NIS1 creó un Grupo de Cooperación que comenzó a funcionar según lo establecido por una Decisión de la Comisión de febrero de 2017 (Decisión (UE) 2017/179 de la Unión Europea). Pero, al quedar derogada por la publicación de la NIS2, en el articulado de esta se recrea otra vez este Grupo con idéntico fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y reforzar la confianza y seguridad entre ellos (10).

Integran el Grupo representantes de los Estados miembros, de la Comisión Europea, que se encarga de la secretaría, y de la Agencia de la Unión Europea para la ciberseguridad (ENISA). Además, pueden participar como observadores invitados otros organismos y entidades incluyendo a representantes del Parlamento Europeo, autoridades europeas de supervisión y partes interesadas relevantes como las empresas privadas o expertos en ciberseguridad.

Entre las múltiples funciones que la Directiva NIS2 asigna al Grupo de Cooperación se encuentran facilitar orientación a los países para trasponer e implementar correctamente la Directiva, coordinar respuestas ante vulnerabilidades e incidentes graves, contribuir a las capacidades de ciberseguridad en la Unión mediante un programa de desarrollo de capacidades en el que participe personal de las autoridades competentes o de los CSIRT, debatir y llevar a cabo periódicamente una evaluación de la situación de las ciberamenazas o incidentes, compartir buenas prácticas e información con las instituciones, órganos y organismos pertinentes de la Unión, realizar evaluaciones conjuntas del riesgo de las cadenas de suministro críticas y proporcionar orientación estratégica a la red de CSIRT y a EU-CyCLONe sobre cuestiones emergentes específicas (10).

5.6. LA DEFENSA EN LA UNIÓN EUROPEA

La invasión rusa de Ucrania significó el regreso de la guerra a suelo europeo: después de 80 años de paz, con la única excepción de la guerra de los Balcanes, contienda étnica y religiosa en la que la entonces Comunidad Europea se implicó aportando fuerzas a los cascos azules de la ONU, y tras haber dejado atrás la Guerra Fría, vuelve a plantearse la necesidad de una defensa de Europa que garantice la seguridad y la autonomía del continente.

Transcurridos ya varios años de conflicto han surgido otras amenazas que, impactando en el contexto estratégico actual, para algunos un nuevo orden mundial, requieren que Europa sea capaz de protegerse a sí misma, así como a sus valores y ciudadanos, en un mundo de inestabilidad creciente, necesidad que puede satisfacerse mediante dos enfoques aparentemente similares pero diferentes: defensa de Europa o Europa de la defensa (2).

5.6.1. Defensa de Europa

La defensa de Europa, entendida como defensa territorial y colectiva contra una agresión armada, es en la actualidad una realidad basada en dos pilares. El primero de ellos lo constituye la conocida cláusula de defensa mutua recogida en el artículo 42 (7) del Tratado de la Unión Europea de 1992 que establece: "si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas" (17).

El segundo de los pilares de la defensa de Europa lo configura la cooperación Unión

Europea-OTAN, cuyos cimientos se construyeron en el año 2003, en los denominados "Acuerdos Berlín Plus" por los que se establecían las bases para que la Alianza apoyara las operaciones dirigidas por la Unión Europea en las que no participe la OTAN en su conjunto.

Posteriormente, en el nuevo Concepto Estratégico de la Alianza, adoptado en la Cumbre de Lisboa en 2010, se reconoce la complementariedad OTAN-Unión Europea, ratificada en la celebrada en Varsovia (2016) donde las dos organizaciones identificaron áreas para fortalecer la cooperación (amenazas híbridas, ciberseguridad, ...) recogidas en 42 medidas aprobadas ese mismo año por los ministros de Asuntos Exteriores de la OTAN y posteriormente ampliadas en diciembre de 2017 hasta un número de 74.

Asimismo, este pilar se ve reforzado por el hecho de que 23 de los 27 Estados miembros de la Unión pertenecen a la OTAN, de forma que están amparados por la cláusula de asistencia mutua recogida en el artículo 5 del Tratado del Atlántico Norte, donde se establece que un ataque a un Estado miembro de la OTAN, en Europa o América del Norte, se considerará contra todos ellos y, en consecuencia, también invocando al artículo 51 de la Carta de las Naciones Unidas, se tomarán individualmente y en concierto con los demás las acciones que se considere necesarias, incluido el uso de fuerza armada, para restaurar y mantener la seguridad del área del Atlántico Norte (2) (18).

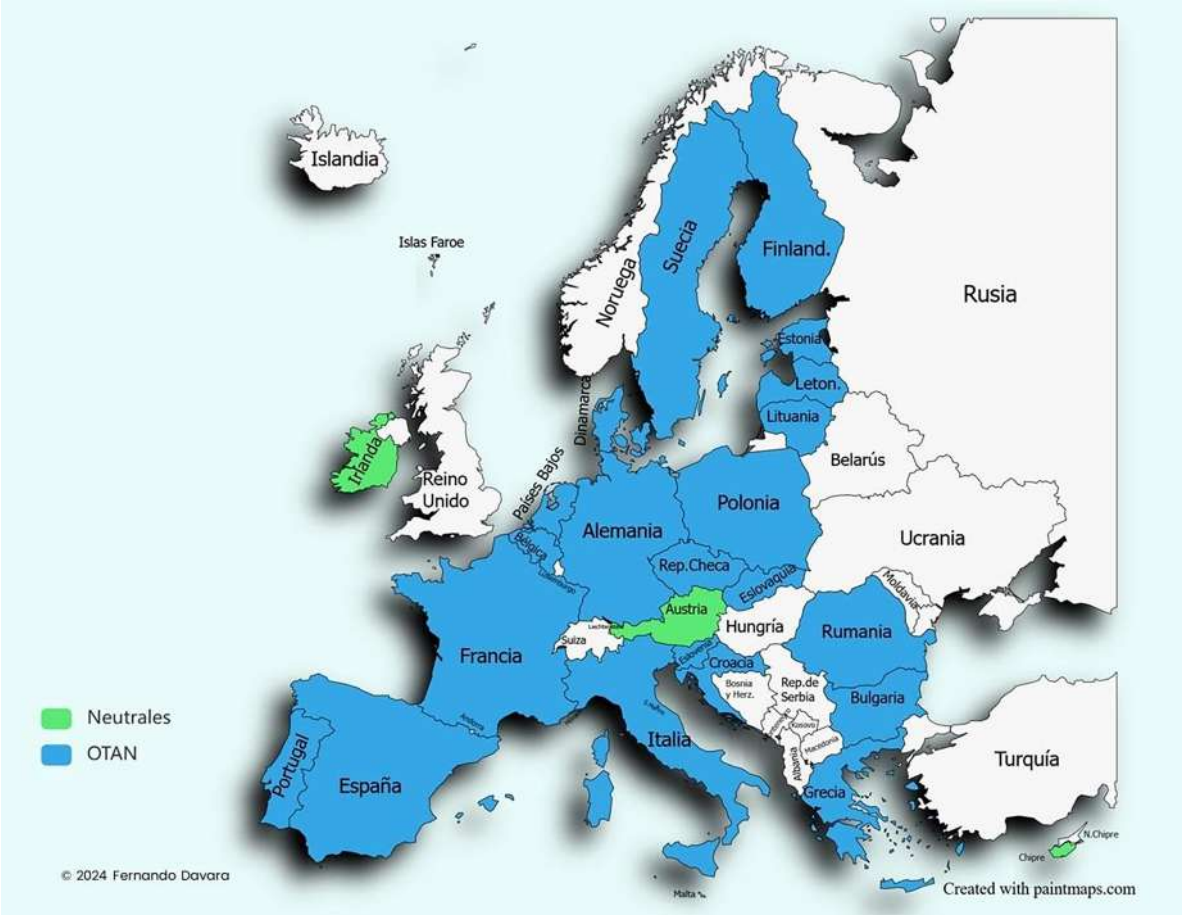


Figura 5.4.
Estados miembros de la Unión Europea.
Elaboración propia.

5.6.2. Europa de la defensa

Si en lugar de la defensa de Europa se hace referencia a la Europa de la defensa, es decir la creación de una Defensa europea, común y a la vez única, la realidad es bastante diferente a la anterior. Los importantes desafíos estratégicos de seguridad y defensa a los que se enfrenta Europa demandan decisiones unificadas y conjuntas que permitan dar respuesta de forma eficaz y eficiente a las amenazas comunes, el fortalecimiento de la soberanía y autonomía colectivas, y la optimización de los recursos disponibles.

En principio podría argumentarse que ya en 1999 se dieron pasos para lograr una cierta autonomía con la creación de la Política Exterior de Seguridad y Defensa (PESD) cuya denominación cambió con el Tratado de Lisboa de 2009, pasando a ser la Política Común de Seguridad y Defensa (PCSD) como parte integrante de la Política Exterior y de Seguridad Común (PESC).

Sin embargo, la PCSD, a pesar de sus avances, no puede considerarse como el núcleo de la Europa de la defensa. Desde su institución se ha mantenido el objetivo, expuesto en el Título V del Tratado, de dotar a la Unión de capacidad operativa para llevar a cabo operaciones en el exterior, cuya finalidad sea garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional; es decir se trata de una política europea de seguridad y no de una Europa de la defensa.

Asimismo, el propio articulado del Tratado de Lisboa (art. 42) reconoce esta diferencia pues si bien señala que la PESD incluirá la definición progresiva de una política común de defensa de la Unión, y que esta conducirá a una defensa común una vez que el Consejo Europeo lo decida por unanimidad, también matiza que será sin que afecte al carácter específico de la política de seguridad y de defensa de determinados Estados miembros, respetando las obligaciones derivadas del Tratado del Atlántico Norte para aquellos que consideran que su defensa común se realiza dentro de la OTAN. Es decir, se trataría de una defensa común no colectiva donde la soberanía nacional prevalece sobre la europea.

En la última década se han puesto en marcha algunas iniciativas institucionales como por ejemplo la Coordinación Estructurada Permanente de Defensa (PESCO)[10], creada por el Tratado de Lisboa, sin activar hasta 2017, la cual permite que los Estados miembros de la Unión colaboren en proyectos específicos de capacidades de Defensa, o el Fondo Europeo de Defensa (FED), adoptado en 2018 como un componente de la PCSD, con el objetivo de coordinar y aumentar la cooperación e inversión nacional en investigación en materia de Defensa y mejorar la interoperabilidad entre las Fuerzas Armadas nacionales.

La invasión de Ucrania por parte de Rusia el 24 de febrero de 2022 y posteriormente el nuevo panorama estratégico dieron lugar a una llamada de atención sobre la defensa de Europa que pasó a ser una prioridad ante la preocupación por las carencias que presenta, aprobándose diferentes iniciativas e instrumentos para llenar los vacíos.

Así, en marzo del 2022, tras dos años de negociaciones los Estados miembros de la Unión adoptaron la denominada "Brújula estratégica en materia de seguridad y defensa (Unión Europea, 7371/22, 2022)" un extenso documento donde se recoge un análisis del entorno estratégico global y un listado de propuestas concretas desglosadas en cuatro apartados: actuar, asegurar, invertir y cooperar.

10. Cooperación Estructurada Permanente (PESCO, Permanent Structured Cooperation): instrumento recogido en el Tratado de Lisboa (artículos 42 y 46) donde los Estados miembros participantes planifican, desarrollan e invierten en el desarrollo conjunto de capacidades de Defensa mejorando la preparación operativa. Creado por Decisión (PESC) 2017/2315 del Consejo (11 diciembre 2017).

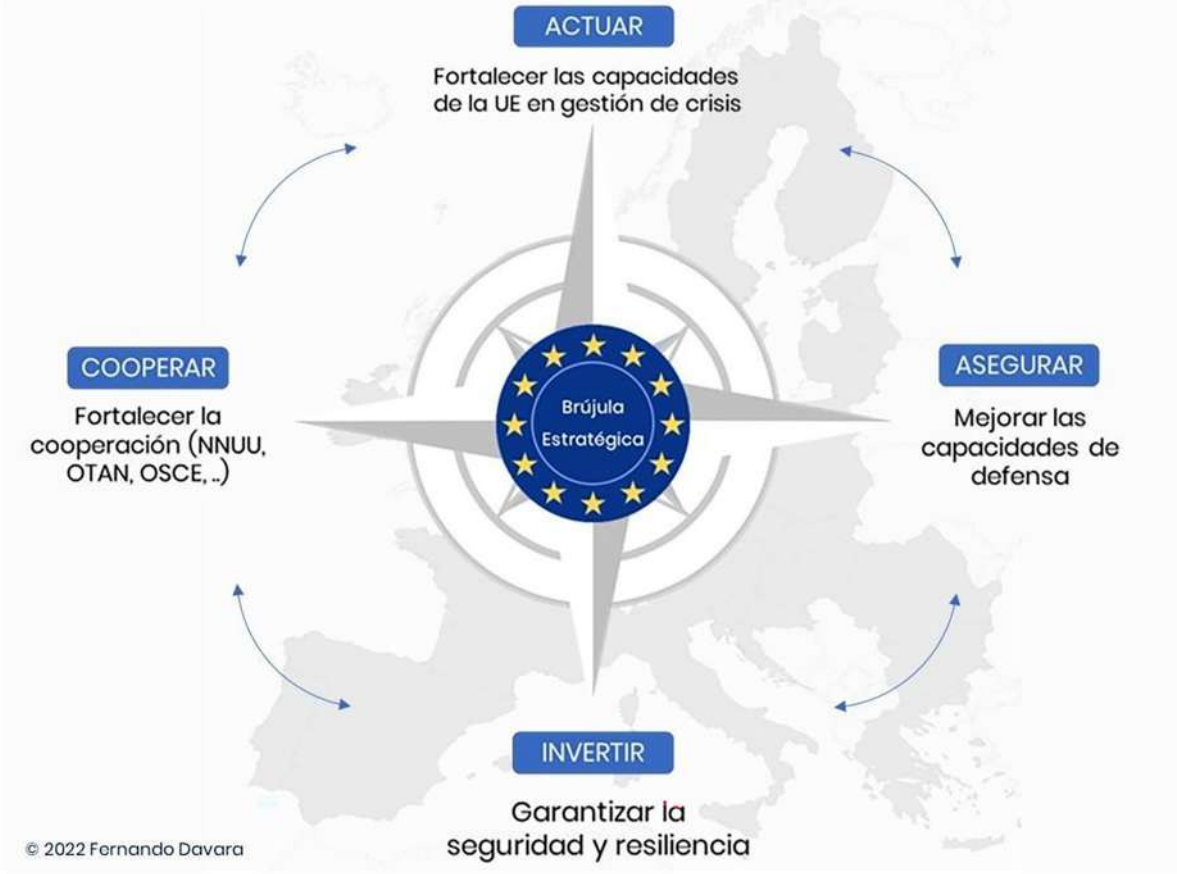


Figura 5.5.
Pilares de la Brújula Estratégica de la Unión Europea.
Elaboración propia, derivada de Unión Europea, 7371/22, 2022 (19).

Sin embargo, aun considerando que constituye un gran avance, tampoco parece que se trate de la base para instaurar la Europa de la Defensa. De su lectura, a pesar de su ambigüedad, puede deducirse que la seguridad colectiva sigue basada en la OTAN, consolidada con el pilar europeo de la defensa común.

Otras iniciativas son el Libro Blanco de la Defensa Europea (White Paper for European Defence - Readiness 2030, 12 march 2025) que define el marco estratégico en el que los Estados miembros deben invertir en Defensa con medidas concretas para pasar de objetivos políticos expresados en términos generales a objetivos específicos y cuantificables, y constituir un elemento de planificación de la Defensa.

Y finalmente, el Parlamento Europeo en la resolución 2025/2565 (RSP) aprobada el 12 de marzo de 2025, instó a la Unión Europea a actuar urgentemente para garantizar su propia seguridad lo cual requiere reforzar sus asociaciones con socios afines y reducir significativamente su dependencia de terceros países en materia de defensa.

En conclusión, los importantes acontecimientos de los últimos años han revitalizado el debate sobre la defensa de Europa, pero, la Europa de la defensa demanda el compromiso de los Estados miembros tratando de aunar los intereses de los 27, tanto europeístas y atlantistas como neutrales, para compartir amenazas y disponer de los medios para defenderse de ellas. Es decir, una defensa no solamente común sino también única basada en una verdadera política de defensa y no, como actualmente, en un componente de la política exterior (2).

5.7. POLÍTICA EUROPEA DE CIBERDEFENSA

De lo expuesto en los apartados anteriores se deduce que la ciberseguridad ha sido desde hace años una cuestión prioritaria para la Unión Europea como lo muestran las numerosas iniciativas adoptadas en forma de reglamentos, directivas, regulaciones, etc. Sin embargo, al ser la defensa, y por ello la ciberdefensa, responsabilidad de los Estados, hasta la segunda década de este siglo la contribución en este ámbito se había limitado a apoyar la cooperación entre los Estados miembros, como se expresa por ejemplo en la Directiva NIS2, sin incluir la ciberdefensa entre las actividades de la Unión Europea.

No ha sido hasta el año 2013 cuando en el marco de la primera Estrategia de ciberseguridad de la Unión (6) se incluye por primera vez el concepto de ciberdefensa en las actividades de la Unión Europea. En su apartado 2.3 (Desarrollo de una política y de capacidades de ciberdefensa en el marco de la Política Común de Seguridad y Defensa (PCSD)) se determina que los esfuerzos de ciberseguridad de la Unión Europea entrañan asimismo una dimensión de ciberdefensa que se deben apoyar con actividades de investigación y desarrollo y una mayor cooperación entre las administraciones públicas, el sector privado y la comunidad académica de la Unión Europea (20).

Asimismo, se indica que, para evitar duplicaciones, la Unión Europea examinará de qué modo pueden ella y la OTAN aunar sus esfuerzos para aumentar la resiliencia de infraestructuras críticas públicas, de defensa y de información de las que dependen los miembros de ambas organizaciones (20).

En ese mismo apartado se insta a la Alta Representante en la época a centrar la atención en evaluar los requisitos operativos de ciberdefensa de la Unión Europea y promover el desarrollo de sus capacidades y tecnologías de ciberdefensa en todos sus aspectos, elaborar un marco político de ciberdefensa de la Unión Europea para proteger las redes dentro de las misiones y operaciones de la PCSD, promover el diálogo y la coordinación entre las esferas civil y militar de la Unión Europea y garantizar el diálogo con los socios internacionales, entre ellos la OTAN, otras organizaciones internacionales y centros de excelencia plurinacionales con el fin de conseguir auténticas capacidades de defensa, determinar las áreas de cooperación y evitar la duplicación de esfuerzos, invitando a los Estados miembros y a la Agencia Europea de Defensa a colaborar en estas actividades (20).

En cumplimiento de este mandato y de acuerdo con las Conclusiones del Consejo Europeo de noviembre de 2013 (20), esta institución invitaba a la Alta Representante, en cooperación con la Agencia Europea de Defensa y la Comisión Europea, a presentar en 2014 un Marco[11] Político de Ciberdefensa de la Unión Europea para promover:

- El desarrollo de las capacidades, la investigación y las tecnologías de ciberdefensa de los Estados miembros mediante el desarrollo y la aplicación de una hoja de ruta integral para fortalecer las capacidades de ciberdefensa.
- La protección reforzada de las redes de comunicación que apoyan las estructuras, misiones y operaciones de la PCSD.
- La integración de la ciberseguridad en la gestión de crisis de la Unión Europea.
- La sensibilización mediante la mejora de las oportunidades de formación, educación y ejercicios para los Estados miembros.

11. Un marco o *framework* (marco de trabajo, en el documento original en inglés) caracteriza un conjunto estandarizado de conceptos, prácticas y criterios que componen un esquema o estructura real o conceptual destinado a enfocar un tipo de tema o problema en particular y servir como referencia para afrontar y resolver nuevos problemas de índole similar.

- Las sinergias con las políticas cibernéticas más generales de la Unión Europea y con todos los demás actores y agencias pertinentes en Europa, como la Agencia de Seguridad de las Redes y de la Información de la Unión Europea.
- La cooperación con los socios internacionales pertinentes, en particular con la OTAN, según corresponda (20).

Algunos días después, el Consejo Europeo en su reunión del 19/20 de diciembre de 2013, reconociendo que las dimensiones de seguridad interior y exterior de Europa están cada vez más interrelacionadas, y con objeto de que la UE y sus Estados miembros puedan responder a los nuevos retos de seguridad, en consonancia con los esfuerzos de la OTAN, reiteraba su invitación anterior solicitando el Marco Político de Ciberdefensa de la UE en 2014, basado en una propuesta del Alto Representante, en cooperación con la Comisión y la Agencia Europea de Defensa (20).

Esta invitación se plasmó en noviembre de 2014 en el documento denominado Marco Político de Ciberdefensa de la Unión Europea (CDPF, Cyber Defence Policy Framework) adoptado por el Consejo el 18 de noviembre de 2014 y elaborado conjuntamente por la Comisión Europea, la Agencia Europea de Defensa y el Servicio Europeo de Acción Exterior (SEAE), con el doble objetivo de dar respuesta a las solicitudes de las mencionadas *Conclusiones del Consejo Europeo y del Consejo*, así como de abordar los aspectos de ciberdefensa de la *Estrategia de Ciberseguridad de la Unión Europea* (2013), entonces en vigor (21).

En él se identifican cinco prioridades de esfuerzos específicos con el fin de desarrollar estrategias viables e identificar a las principales partes interesadas responsables de su implementación:

1. Apoyar el desarrollo de las capacidades de ciberdefensa de los Estados miembros relacionadas con la PCSD.
2. Mejorar la protección de las redes de comunicación de la PCSD utilizadas por las entidades de la Unión Europea.
3. Fomento de la cooperación cívico-militar y de las sinergias con políticas cibernéticas más amplias de la Unión Europea, con las instituciones y organismo correspondientes de la Unión, así como con el sector privado.
4. Mejorar la formación, educación y las oportunidades de realizar ejercicios conjuntos.
5. Incrementar la cooperación con los socios internacionales pertinentes, en particular la OTAN (21).

Con este fin, se expresa que los objetivos de la ciberdefensa deberán hallarse mejor integrados en los mecanismos de gestión de crisis de la Unión y que para abordar los efectos de las crisis cibernéticas podrán aplicarse, según proceda, las disposiciones pertinentes del Tratado de la Unión Europea (cláusula de defensa mutua) y del Tratado de Funcionamiento de la Unión Europea (cláusula de solidaridad). Artículo 222 del TFUE y el artículo 42.7 del TUE, teniendo en cuenta debidamente el artículo 17 del TUE.

Estas disposiciones muestran claramente el compromiso de la Unión de aprovechar los mecanismos de gestión de crisis establecidos en el Tratado de Lisboa para fines de ciberdefensa.

Con el fin de evaluar el grado de cumplimiento del Marco en él se estipulaba que debería presentarse al Grupo Político-Militar, al Comité Político y de Seguridad y a otros Grupos pertinentes del Consejo un informe de situación semestral que incluyera las cinco prioridades.

De los primeros informes se dedujo que su aplicación había contribuido a mejorar significativamente alguna de sus áreas, como la cooperación institucional y las capacidades en ciberdefensa de los Estados miembros. Sin embargo, a partir de lo expuesto en los mencionados informes semestrales, y teniendo en consideración otras diferentes iniciativas que se fueron adoptando en el ámbito de la Seguridad y la Defensa de la Unión, como la Revisión Anual Coordinada

de la Defensa (CARD)[12], la Cooperación Estructurada Permanente (PESCO) con sus proyectos PESCO[13], o la creación del Fondo Europeo de Defensa[14], los Estados miembros pidieron una actualización del Marco.

Su puesta al día se caracterizó por el nuevo Marco Político de Ciberdefensa de la Unión Europea (actualización de 2018) (22) adoptado por el Consejo en su sesión celebrada el 19 de noviembre de 2018, donde se tienen en cuenta los cambios en los retos de ciberseguridad acaecidos desde la adopción del marco inicial, en 2014.

Un primer aspecto a destacar es que por primera vez en los diferentes documentos de la Unión se reconoce el ciberespacio como el quinto dominio de operaciones, junto con los de tierra, mar, aire y espacio, concluyendo que la implementación con éxito de las misiones y operaciones de la Unión Europea depende cada vez más del acceso ininterrumpido a un ciberespacio seguro y, por lo tanto, requiere capacidades operativas cibernéticas sólidas y resilientes (22).

El objetivo del Marco político actualizado, basado en la aplicación del de 2014, es seguir desarrollando la política de ciberdefensa de la Unión Europea, teniendo en cuenta los avances en otros ámbitos políticos. De igual forma que el anterior, el actual identifica unas áreas prioritarias para la ciberdefensa, en esta ocasión seis, y aclara las funciones de los diferentes actores europeos, respetando plenamente las responsabilidades y competencias de los agentes y de los Estados miembros, así como el marco institucional de la Unión Europea y su autonomía en la toma de decisiones.

Tales áreas prioritarias para la ciberdefensa se sintetizan en las siguientes:

1. Apoyar el desarrollo de las capacidades de ciberdefensa de los Estados miembros, abordando aspectos como doctrina, liderazgo, organización, personal, formación, industria, tecnología, infraestructura, logística e interoperabilidad. Para ello los Estados miembros deben intensificar sus esfuerzos para ofrecer una capacidad eficaz de ciberdefensa.
2. Mejorar la protección de los sistemas de comunicación e información de la PCSD utilizados por las entidades de la Unión, con el objetivo de optimizar la resiliencia de sus redes, centrándose en la prevención, detección, y respuesta, el conocimiento de la situación, el intercambio de información y los mecanismos de alerta temprana. En este contexto, podría considerarse la posibilidad de una cadena de mando unificada con el objetivo de mejorar la resiliencia de las redes utilizadas para la PCSD.
3. Promoción de la cooperación civil-militar, entre el ámbito civil y el militar en los casos de tecnologías similares que proporcionen soluciones duales. Sin perjuicio de la legislación propia de los Estados miembros, la cooperación civil-militar en el ámbito cibernético puede considerarse, entre otras cosas, para el intercambio de mejores prácticas, alerta temprana, evaluación de riesgos de respuesta a incidentes y sensibilización, y para entrenamientos y ejercicios.

12. Revisión Anual Coordinada de la Defensa (CARD, Coordinated Annual Review on Defence), Ciclo bienal de identificación de oportunidades de cooperación en materia de Defensa. Se lleva a cabo bajo la coordinación de la Agencia Europea de Defensa (EDA) y la participación del Servicio Europeo de Acción Exterior (SEAE) y del Estado Mayor de la Unión Europea (EUMS).
13. Proyectos PESCO; en el marco de la PESCO están diseñados para proporcionar capacidades para el uso de los Estados miembros, incluido el apoyo a las operaciones y misiones de la Política Común de Seguridad y Defensa (PCSD), y brindan a los Estados miembros participantes la oportunidad de cooperar en todos los ámbitos de la Defensa incluyendo entre ellos varios de ciberdefensa.
14. Fondo Europeo de Defensa; European Defence Fund (FED); Instituido el 2016 para apoyar la investigación y el desarrollo tecnológico en materia de Defensa y fomentar una base industrial innovadora y competitiva conjunta de capacidades prioritarias en materia de Defensa.

4. Investigación y tecnología, como una importante dimensión para contribuir al desarrollo de las capacidades de ciberdefensa al identificar oportunidades para los esfuerzos e inversiones de doble uso, ya sea a nivel nacional, multinacional o financiado por la Unión Europea, apoyando la participación con las pequeñas y medianas empresas, y garantizar que Europa sea capaz de mantenerse al día con los competidores internacionales en materia de cibertecnología.
5. Mejorar las oportunidades de educación, formación y ejercicios en ciberdefensa de los Estados miembros, para hacer frente a las ciberamenazas y desarrollar una cultura común de ciberdefensa en toda la Unión Europea. También es necesario mejorar las oportunidades de ejercicios de ciberdefensa para los actores civiles y militares de la PCSD con el objetivo de desarrollar el conocimiento común y la comprensión de la ciberdefensa.
6. Mejorar la cooperación con los socios internacionales garantizando el diálogo con ellos, en particular la OTAN, con el fin de contribuir al desarrollo de capacidades efectivas de ciberdefensa, tratando de evitar duplicaciones innecesarias y garantizar la coherencia y la complementariedad de esfuerzos (22).

De igual forma que en la versión 2014 en el nuevo documento se estipulaba que debe presentarse un informe anual de situación de las seis áreas descritas considerando esencial que, a medida que se desarrolla la amenaza cibernética, se identifiquen nuevos requisitos de ciberdefensa a incluir en el Marco de la Política de Ciberdefensa cuya próxima revisión debería ser a más tardar a mediados de 2022, en estrecha consulta con los Estados miembros (22).

Sin embargo, en ese período se produjeron dos hechos importantes: la presentación por la Comisión y el Servicio Europeo de Acción Exterior de la nueva Estrategia de ciberseguridad de la Unión Europea (2020) y la adopción por el Consejo Europeo de la Brújula Estratégica (2022).

En el primero de estos documentos, la Estrategia, se estima que la Unión Europea y los Estados miembros deben aumentar su capacidad para prevenir y responder a las ciberamenazas, de acuerdo con el Nivel de Ambición de la Unión Europea derivado de la Estrategia Global de la Unión de 2016 (14149/16).

Para ello, se demanda que la Alta Representante, en colaboración con la Comisión, presente otra revisión del Marco Político de Ciberdefensa para reforzar la coordinación y la cooperación entre los actores de la Unión Europea[15], así como con y entre los Estados miembros, incluso en lo que respecta a las misiones y operaciones de la Política Común de Seguridad y Defensa (PCSD). Esta revisión debe servir de base para la próxima Brújula Estratégica, garantizando que la ciberseguridad y la ciberdefensa se integren en mayor medida en la agenda más amplia de seguridad y defensa (7).

Por su parte en el documento Brújula Estratégica para la Seguridad y la Defensa se señala que ante la necesidad de mejorar la capacidad para anticiparse a las amenazas, garantizar el acceso seguro a dominios estratégicos y proteger a los ciudadanos, se continuará desarrollando la política de ciberdefensa de la Unión Europea para estar mejor preparados ante los ciberataques y responder mejor a ellos, mejorando así la capacidad de prevenir, detectar, defenderse, recuperarse y disuadir de los ciberataques dirigidos a la Unión Europea y a sus Estados miembros (19).

Finalmente, en mayo del 2022, en el documento que recoge las Conclusiones del Consejo sobre el desarrollo de la postura cibernética de la Unión Europea (9364/22), los Estados miembros invitaron al Alto Representante junto con la Comisión a complementar el desarrollo de una postura cibernética de la Unión Europea presentando una propuesta ambiciosa para una Política de Ciberdefensa de la Unión en 2022,

15. Entre estos actores en la Estrategia se destaca el SEAE, el Estado Mayor Militar de la UE (EMUE), la Escuela Europea de Seguridad y Defensa (ESDC), la Comisión y las agencias de la UE, en particular la Agencia Europea de Defensa.

con el resultado de que en noviembre de ese año se presentó la primera y actual definición de Política de ciberdefensa de la Unión Europea.

Este hecho tuvo lugar el 10 de noviembre de 2022, cuando la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una Comunicación Conjunta al Parlamento Europeo y al Consejo sobre la Política de ciberdefensa de la Unión Europea (23) para abordar el deterioro del entorno de seguridad tras la agresión de Rusia contra Ucrania y fortalecer la capacidad de la Unión Europea para proteger a sus ciudadanos e infraestructuras.

Esta política está diseñada para impulsar las capacidades de ciberdefensa, mejorar la coordinación entre las comunidades cibernéticas de la Unión Europea y reforzar la Base Tecnológica e Industrial de la Defensa Europea (BITDE) Unión Europea (23).

En el documento se detalla la estructura de la política de ciberdefensa de la Unión Europea basada en cuatro pilares que abarcan una amplia gama de iniciativas que ayudarán a la Unión Europea y a los Estados miembros a estar mejor capacitados para detectar, disuadir y defenderse de los ciberataques:

- Actuar juntos para reforzar la ciberdefensa de la Unión Europea: por medio de este pilar se busca convertir la ciberdefensa en un elemento autónomo, promoviendo al mismo tiempo mecanismos de coordinación diversificados entre los Estados miembros y la Unión Europea. Para ello la Unión reforzará sus mecanismos de coordinación entre los agentes nacionales y de la Unión Europea en materia de ciberdefensa, para aumentar el intercambio de información y la cooperación entre las comunidades de ciberseguridad militares y civiles, y seguir apoyando las misiones y operaciones militares de la PCSD.
- Proteger el ecosistema de defensa de la Unión Europea: pilar orientado a la protección del ecosistema de defensa mediante la prevención, abordando las deficiencias en la normalización y certificación de la ciberseguridad, tanto en la dimensión militar como en la civil. Dado que incluso los componentes de *software* no críticos pueden utilizarse para llevar a cabo ciberataques contra empresas o gobiernos, incluido el sector de la defensa es necesario seguir trabajando en la normalización y certificación de la ciberseguridad para proteger tanto el ámbito militar como el civil.
- Invertir en capacidades de ciberdefensa: ante la necesidad urgente de aumentar significativamente la financiación al ser impracticable que un solo Estado miembro satisfaga las demandas financieras de forma unilateral los Estados miembros deben aumentar significativamente las inversiones en capacidades militares modernas de ciberdefensa mediante un enfoque colaborativo, utilizando las autoridades nacionales, las plataformas de cooperación y los mecanismos de financiación disponibles a nivel de la Unión, como el Fondo Europeo de Defensa (FED) y la CEP, así como Horizonte Europa y el Programa Europa Digital y realizando formación y ejercicios de ciberdefensa específicos de la Unión Europea para fomentar las sinergias entre el mundo académico y la innovación en el ámbito cibernético.
- Asociarse para hacer frente a los retos comunes: este cuarto y último aborda las relaciones de la Unión con sus socios, centrándose en la convergencia y la coherencia. Sobre la base de la seguridad y la defensa existentes, así como de los diálogos cibernéticos con los países socios, la Unión Europea tratará de establecer asociaciones adaptadas en el ámbito de la ciberdefensa. Los esfuerzos se centrarán en establecer o fortalecer asociaciones adaptadas a la voluntad política de los beneficiarios, fomentando un diálogo basado en la confianza mutua, centrándose en tres áreas: las relaciones Unión Europea-OTAN, los socios afines y los países socios. Esta estrategia integral subraya el compromiso de la Unión Europea con una política de ciberdefensa sólida y coordinada, que integre múltiples sectores y fomente la colaboración internacional (23).

En síntesis, la nueva política exige inversiones en capacidades de ciberdefensa de espectro completo y fortalecerá la coordinación y la cooperación entre las comunidades cibernéticas militares y civiles de la Unión Europea, fortalecerá la cooperación con el sector privado y la gestión eficaz de crisis de tecnologías de la información dentro de la Unión. También ayudará a reducir las dependencias estratégicas de tecnologías cibernéticas críticas y fortalecerá la Base Industrial de Tecnología de Defensa Europea (EDTIB), impulsando la formación, atracción y retención del talento cibernético (23).

A tal efecto, el Consejo instó al Alto Representante y a la Comisión Europea a elaborar un plan de implementación a aprobar en el segundo trimestre de 2023. Además, se alentó a los Estados miembros a adoptar las recomendaciones esbozadas y también se les instó a adoptar un mayor nivel de ambición y dedicación política para maximizar la eficacia de la política de ciberdefensa (23).

Esta Política de ciberdefensa se ha ido mejorando sucesivamente por medio de documentos e iniciativas como las Conclusiones del Consejo sobre Política de ciberdefensa (9618/23), de mayo de 2023, las propuestas presentadas por la presidenta de la Comisión Europea, en su discurso de julio de 2024 sobre las Directrices Políticas para la Próxima Comisión Europea (2024-2029) o el Libro Blanco sobre la preparación europea para la defensa 2030 (24).

También puede considerarse una mejora la promulgación de la Ley de Ciberseguridad (25) en diciembre de 2024 pues si bien los mecanismos que establece son de carácter civil, tanto el Sistema Europeo de Alerta de Ciberseguridad como el Mecanismo de Emergencia, recogidos en ella, pueden apoyar a la comunidad de ciberdefensa al beneficiarse de unas capacidades civiles más sólidas de detección resiliencia y complementar la asistencia prestada en el contexto de la PESC y la PCSD, en particular a través de los Equipos de Respuesta Rápida.

5.8. CONCLUSIONES Y REFLEXIONES

Una de las primeras conclusiones que se derivan de este análisis es que la política de ciberdefensa de la Unión Europea ha ido evolucionando de forma paulatina desde sus primeros pasos en el año 2013, adquiriendo un protagonismo cada vez mayor con importantes avances hasta llegar a la definición de una Política de Ciberdefensa orientada a mejorar la capacidad de la Unión para detectar, disuadir y defenderse de los ciberataques. Sin embargo, queda mucho camino que recorrer.

Acabando la primera década de este siglo, al entrar en vigor el Tratado de Lisboa (2009), la Unión Europea se otorgó una personalidad jurídica propia y estableció unas nuevas estructuras institucionales para hacer frente a los modernos riesgos y amenazas, suprimiendo la estructura en pilares introducida en 1993 e introduciendo cambios importantes en la PESC, entre ellos la actualización de la antigua PESD que pasó a ser la PCSD, reforzando sus capacidades e instrumentos de actuación, introduciendo la posibilidad de que los Estados miembros participen voluntariamente en la Cooperación estructurada permanente para intensificar gradualmente la cooperación en materia de defensa con el fin de ofrecer las capacidades necesarias para las misiones más exigentes.

Sin embargo, en esta nueva época, en el ámbito del ciberespacio la preocupación y participación de la UE se limitaba a fines económicos y de seguridad, sin considerar la Defensa, como muestra la creación en 2004 de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) que se justificaba para establecer un elevado nivel de seguridad de las redes e información en la Unión y también para el desarrollo de una cultura de la seguridad de ambos activos en beneficio de los ciudadanos, los consumidores, las empresas y las administraciones públicas.

Es a partir de los ciberataques de abril de 2007, considerados por algunos como los primeros ataques cibernéticos lanzados por Estados, cuyos objetivos fueron los sitios web de diversas organizaciones de Estonia, como Parlamento, bancos, ministerios, etc., cuando se empezó a reflexionar sobre los riesgos inherentes a esta nueva amenaza.

La Unión Europea también fue consciente de ello tomando medidas para hacer frente a los nuevos desafíos cibernéticos, pero centradas principalmente en la identificación y protección de las denominadas infraestructuras críticas europeas, que posteriormente se ampliaron al resto de Estados miembros, una vez más dirigidas a salvaguardar redes e información.

El año 2013 marcó un punto de inflexión con la publicación de la primera Estrategia de ciberseguridad de la UE (un ciberespacio abierto, seguro y protegido) donde se incluye la ciberdefensa entre las cinco prioridades estratégicas de la Unión recomendando el desarrollo de una política y medios de ciberdefensa en conjunción con la política común de seguridad y defensa (PCSD).

A partir de entonces, reconociendo el carácter multidimensional de la ciberseguridad, el tratamiento de la ciberdefensa se va plasmando en diferentes iniciativas y documentos, entre los que destacan los Marcos Políticos de Ciberdefensa (2014 y 2018), la nueva Estrategia de Ciberseguridad de la UE (2020) y la Política de ciberdefensa de la UE (2022).

Pero el entorno geopolítico actual es muy diferente al de décadas anteriores. En estos últimos años se han ido produciendo acontecimientos de importancia, como la pandemia global, la invasión de Ucrania, el impacto de la tecnología en los conflictos armados, las relaciones transatlánticas, etc., complementados en el ámbito del ciberespacio por el incremento de actores, entre ellos los Estados, y de ataques cibernéticos cada vez más sofisticados, que han alterado el panorama geopolítico caracterizado por una mayor polarización e inestabilidad global, con consecuencias importantes en términos de seguridad y defensa, afectando también a la ciberseguridad y ciberdefensa europeas.

En este contexto, aun reconociendo que se han producido avances importantes, parece lógico estimar que en el escenario geopolítico actual la política europea de ciberdefensa no es lo suficientemente madura como para hacer frente a los crecientes nuevos desafíos, al existir deficiencias estructurales e importantes diferencias entre los Estados miembros que dificultan la creación de un ecosistema de ciberdefensa unificado.

Un primer aspecto a considerar es la limitación impuesta por los Tratados en cuanto a la soberanía de los Estados miembros en materia de seguridad y defensa, y por ello en ciberdefensa, lo cual contribuye a levantar barreras basadas en las diferentes prioridades políticas, o en las diferencias en capacidades, preparación y experiencia, la financiación e inversión muy desiguales, la falta de consenso en el reparto de costes y, no menos importantes, en las reticencias o falta de confianza de algunos Estados sobre el acceso de otros países a redes sensibles, la participación en ellas de personal extranjero o el intercambio de información.

Otro aspecto a considerar, relacionado con el anterior, se refiere a las diferentes responsabilidades del complejo entramado de las instituciones y organismos comunitarios que cooperan en el ámbito de la ciberdefensa, como son la Comisión Europea, el Servicio Europeo de Acción Exterior (SEAE), la Agencia Europea de Defensa, así como de ENISA y de la Agencia de la Unión Europea para la Cooperación Policial (Europol), muchas de cuyas decisiones y recomendaciones se adoptan normalmente por unanimidad de los Estados miembros, cada uno con percepciones diferentes sobre la seguridad y la defensa.

También en este escenario geopolítico actual se acentúa la importancia de la cooperación con la OTAN cuyas capacidades pueden complementarse con las de la ciberdefensa europea, evitando duplicaciones y asegurando una mayor autonomía estratégica lo cual ayudaría a aumentar los medios disponibles para hacer frente a amenazas conjuntas. En este ámbito un

elemento de gran valor es la ciberinteligencia, generada a partir del intercambio de información sobre ciberataques y nuevas amenazas, teniendo siempre en consideración la soberanía de los Estados, en particular los que no pertenecen a la Organización.

Las últimas demandas estadounidenses respecto a la mayor asunción de responsabilidades europeas en el ámbito de la Defensa abarcan también a la ciberdefensa. Esto supone que la Unión debe contraer mayores compromisos y el establecer un reparto eficaz de responsabilidades entre los miembros europeos de la OTAN y la UE, pero también revela que la complementariedad entre ambas organizaciones continúa siendo esencial y la colaboración entre ellas ayudará a la Unión a jugar su papel en el espacio global de la ciberdefensa.

En este espacio de cooperación entre la OTAN y la UE hay un asunto poco tratado, pero de especial importancia para la ciberdefensa. Como se expuso anteriormente, en el caso de que un Estado miembro sea objeto de una agresión armada se aplicaría la cláusula de defensa mutua recogida en el artículo 42 (7) del Tratado de la Unión Europea. Asimismo, si ese Estado fuera uno de los 23 que pertenece también a la OTAN sería de aplicación la similar cláusula de asistencia mutua recogida en el artículo 5 del Tratado del Atlántico Norte.

En ambos casos surge la duda, si la agresión armada se lleva a cabo mediante un ataque con armamento cibernético, ¿serían de aplicación ambas cláusulas y el resto de Estados miembros deberían responder, ayudando y asistiendo con todos los medios a su alcance? A la vista del escaso o nulo interés con que se ha tratado este tema y las diferencias entre los Estados, mencionadas anteriormente, no parece que actualmente exista una voluntad unánime de aplicación de las cláusulas.

Tampoco ahora parece oportuno debatir en la Unión el tratamiento de la denominada ciberdefensa activa, que añade a la protección y resiliencia la neutralización del atacante mediante el uso de contraataques y acciones ofensivas limitadas. Este concepto aparece recomendado en diversos documentos políticos de la Unión Europea, pero, como la actual política de ciberdefensa se basa en la disuasión, antes de llegar a acuerdos sobre su adopción los Estados miembros deberían establecer normativas y competencias jurídicas y políticas sobre su aplicación, con la dificultad añadida de que los Estados neutrales presenten objeciones al entender que puede suponer una militarización del ciberespacio.

Finalmente, no debe olvidarse un aspecto de crucial importancia; en materia de Defensa, y por ello en la ciberdefensa, el activo más importante es el factor humano cuya formación, conocimiento y experiencia constituyen el elemento fundamental que asegura que las capacidades tecnológicas se adecuan y sirven operativamente a las necesidades de este nuevo espacio de conflictos. Esto implica la búsqueda, obtención y retención del talento necesario para mantener un alto nivel de eficiencia en la utilización de forma óptima de las capacidades de ciberdefensa y de eficacia para alcanzar los resultados deseados.

En definitiva, si se desea alcanzar una Política europea de ciberdefensa conjunta, segura y resiliente, es necesario adoptar un enfoque de cooperación multidimensional que abarque esfuerzos políticos, económicos, tecnológicos y de generación y mantenimiento de talento, para adquirir y mejorar las capacidades necesarias que permitan hacer frente a las crecientes amenazas cibernéticas, procurando que las barreras nacionales no dificulten la defensa del entorno sin fronteras que es el ciberespacio común.

5.9. REFERENCIAS BIBLIOGRÁFICAS

1. Gibson W. Neuromancer. New York: An Ace Book; 1984.
2. Davara F. Geopolítica del ciberespacio: las ciberpotencias. Gac. Cult. Ateneo Valladolid [Internet]. 2022;(95):16-21. Disponible en: https://www.ateneodevalladolid.org/wp-content/uploads/GACETA-95-WEB.pdf
3. ISO/IEC. Cybersecurity - Guidelines for Internet security. ISO/IEC 27032:2023 [Internet]. 2023 [citado 22 de mayo de 2025]. Disponible en: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en
4. Davara F. La nueva dimensión de los conflictos. Gac. Cult. Ateneo Valladolid [Internet]. 2025;(103):27-32. Disponible en: https://www.ateneodevalladolid.org/wp-content/uploads/Gaceta-103.pdf
5. Ventre D. Le cyberespace: définitions, représentations. Revue Défense Nationale. 2012;(751):33-8.
6. Unión Europea. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. JOIN(2013)1 final. 2013 feb 7.
7. Unión Europea. Estrategia de ciberseguridad de la Unión Europea para la Década Digital. JOIN(2020)18 final. 2020 dic 16.
8. Davara F. GDPR; el nuevo reglamento de protección de datos de la Unión Europea. Fernando Davara; Reflexiones sobre la sociedad digital [Internet]. 28 de mayo de 2016 [citado 22 de mayo de 2025]. Disponible en: https://fernandodavara.com/gdpr-nuevo-reglamento-proteccion-datos-la-union-europea/
9. Unión Europea. Directiva (UE) 2016/1148. Diario Oficial de la Unión Europea. 2016 jul 19;(194):1-30.
10. Unión Europea. Directiva (UE) 2022/2555. Diario Oficial de la Unión Europea. 2022 dic 27;(333):80-152.
11. Unión Europea. Reglamento (UE) 2019/881. Diario Oficial de la Unión Europea. 2019 jun 7;(151):15-69.
12. Unión Europea. Reglamento (UE) 2025/38. Diario Oficial de la Unión Europea. 2025 enero 15;(32).
13. Unión Europea. Reglamento (CE) n.° 460/2004. Diario Oficial de la Unión Europea. 2004 mar 13;(77):1-11.
14. Unión Europea. Acuerdo CERT (UE) (2018/C 12/01). Diario Oficial de la Unión Europea. 2018 enero 13;(12).
15. Unión Europea. Reglamento (UE) 2021/694. Diario Oficial de la Unión Europea. 2021 mayo 11;(166):1-34.
16. Unión Europea. Reglamento (UE) 2021/887. Diario Oficial de la Unión Europea. 2021 jun 8;(202):1-31.
17. Unión Europea. Tratado de la Unión Europea. Diario Oficial de la Unión Europea. 1992 jul 29;(191):1-112.

18. Organización del Tratado del Atlántico Norte. Tratado del Atlántico Norte. Washington DC; 1949 Apr 4.

19. Unión Europea. Una Brújula Estratégica para la Seguridad y la Defensa. Consejo de la UE. 2022 Mar 21;7371/22.

20. Unión Europea. Conclusiones del Consejo sobre la Política Común de Seguridad y Defensa. EUCO 217/13. 2013 nov 25-26.

21. Unión Europea. Marco político de ciberdefensa de la UE. 2014 nov 17–18;15585/14.

22. Unión Europea. Marco político de ciberdefensa de la UE (actualización 2018). 2018 nov 19;14413/18.

23. Unión Europea. Política de ciberdefensa de la Unión Europea. JOIN(2022)49 final. 2022 nov 10.

24. Unión Europea. Libro blanco conjunto; preparación en materia de Defensa europea 2030. JOIN(2025)120 final. 2025 mar 19.

25. Unión Europea, Reglamento (UE) 2025/38, 2024 por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cibersolidaridad).

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

6

Seguridad en las redes

Xavier Larriva-Novo
Carmen Sánchez-Zas

6.1. LA CIBERSEGURIDAD DESDE UN ENFOQUE HISTÓRICO

El desarrollo de los sistemas de comunicación ha sido un factor clave en la evolución de la sociedad moderna. Desde la invención del telégrafo en el siglo XIX hasta la consolidación de Internet en el siglo XXI, la humanidad ha experimentado una transformación radical en la forma en que intercambia información.

6.1.1. Desarrollo tecnológico en los sistemas de comunicaciones

El concepto de telecomunicaciones se refiere a la transmisión de información a distancia a través de medios electrónicos o electromagnéticos. Su evolución ha estado marcada por hitos tecnológicos fundamentales:

- **El telégrafo (1837)**: considerado el primer sistema de comunicación electrónica, permitió la transmisión de mensajes codificados mediante señales eléctricas a través de cables.
- **El teléfono (1876)**: inventado por Alexander Graham Bell, revolucionó la comunicación al permitir la transmisión de la voz en tiempo real.
- **La radio (1906)**: la transmisión inalámbrica de señales de audio amplió las posibilidades de comunicación masiva.
- **La televisión (1927)**: introdujo la transmisión de imágenes en movimiento, estableciendo una nueva era en la difusión de información.
- **Las redes de datos (década de 1960-1980)**: la creación de redes como ARPANET, precursor de Internet, permitió el intercambio de información entre computadoras, sentando las bases de la era digital.

Cada uno de estos avances fue un paso crucial hacia la interconectividad global que hoy caracteriza a la sociedad de la información.

El auge de Internet ha sido, sin duda, el mayor avance en el desarrollo de los sistemas de comunicación. Su origen se remonta a la década de 1960 con la creación de **ARPANET**, una red diseñada para la comunicación entre universidades y centros de investigación en Estados Unidos. En las décadas siguientes, la expansión de Internet trajo consigo una serie de innovaciones:

- **Protocolo TCP/IP (1983)**: estableció el modelo de comunicación estándar para la interconectividad global de redes.
- ***World Wide Web* (1991)**: creada por Tim Berners-Lee, permitió la navegación de información a través de páginas web.
- **Expansión de la banda ancha (años 2000)**: facilitó una conexión más rápida y estable, impulsando la transformación digital.
- **Redes móviles 3G, 4G y 5G (2000 en adelante)**: permitieron la conectividad inalámbrica en tiempo real y el auge de dispositivos inteligentes.

El diseño de estas infraestructuras fue guiado principalmente por la necesidad de optimizar la transmisión de datos, la accesibilidad y la escalabilidad. Sin embargo, la seguridad no fue una prioridad en sus primeras etapas, lo que generó una serie de vulnerabilidades explotadas con el tiempo (1).

El crecimiento exponencial de las telecomunicaciones ha traído consigo numerosos beneficios, pero también desafíos críticos en términos de seguridad:

- **Interconectividad masiva**: la digitalización ha permitido que millones de dispositivos estén conectados simultáneamente, ampliando la superficie de ataque para cibercriminales.
- **Dependencia de las infraestructuras digitales**: sectores como la banca, la salud y la administración pública dependen de redes de comunicación seguras para su funcionamiento.

- **Evolución del cibercrimen**: la proliferación de ataques informáticos, como el *ransomware* y el *phishing*, ha evidenciado la necesidad de reforzar la seguridad en los sistemas de comunicación.

La falta de previsión en la seguridad de los sistemas de comunicación ha obligado a la industria a desarrollar soluciones posteriores para mitigar estos riesgos. La implementación de cifrado, la autenticación segura y los sistemas de detección de intrusos son ejemplos de las medidas adoptadas para hacer frente a las amenazas actuales (2).

6.1.2. Sistemas no diseñados para ser seguros: evolución histórica y consecuencias

La arquitectura de los sistemas digitales modernos está marcada por un concepto fundacional: fueron diseñados para funcionar en entornos de colaboración, sin considerar la existencia de un posible atacante a los sistemas. Este sesgo de origen no es una deficiencia accidental, sino una característica derivada de decisiones técnicas, institucionales y culturales tomadas en contextos donde la seguridad no era una prioridad.

Michael Warner lo expresa con claridad: la historia de la ciberseguridad no comienza en los años 2000, sino en las décadas de 1960 y 1970, cuando surgieron las primeras preocupaciones sobre los riesgos del uso compartido, la conectividad remota y la falta de control sobre los usuarios y procesos (3). Warner identifica cuatro etapas de toma de conciencia institucional en EE. UU.:

1. Los ordenadores pueden filtrar información sensible (la década de 1960).
2. Los ordenadores pueden ser atacados y sus datos robados (la década de 1970).
3. Los ataques informáticos pueden formar parte del arsenal militar (las décadas de 1980 y 1990).
4. Otros actores pueden atacarnos, y quizá ya lo hacen (de la década de 1990 en adelante).

Cada una de estas ideas fue anticipada teóricamente antes de manifestarse empíricamente. En la década de 1960, los ordenadores eran sistemas centralizados, operados por técnicos especializados en instalaciones cerradas. Sin embargo, con el surgimiento de los sistemas compartidos y las terminales remotas, surgió el problema de la compartición de recursos no controlada. El informe de Willis Ware en 1970, publicado por RAND para el Departamento de Defensa, indicaba que no existía ni podía existir, una solución técnica capaz de garantizar seguridad en un entorno abierto.

Los riesgos no eran abstractos. En 1968, un espía de Alemania Oriental fue capturado trabajando dentro de IBM Alemania, robando información directamente de sistemas informáticos. Fue uno de los primeros casos documentados de espionaje a nivel de computadores.

A inicios de los años 70, los sistemas conectados comenzaron a fallar en las pruebas de seguridad más básicas. Un caso emblemático fue el de la DIA (*Defense Intelligence Agency*), que intentó crear una base de datos con seguridad multinivel. Durante un test de penetración, técnicos de la NSA y contratistas externos lograron tomar control completo del sistema desde una terminal remota.

La expansión de redes interconectadas transformó la seguridad de un problema interno a una cuestión estratégica. El teniente coronel Roger Schell documentó en 1979 cómo los sistemas de la Fuerza Aérea, incluso clasificados, podían ser comprometidos por "fallos deliberados" introducidos durante el desarrollo. El concepto de ataque remoto adquirió una definición operativa (3).

En este contexto surge un episodio que definió la era: el gusano de Morris lanzado en 1988. Diseñado por un estudiante como un experimento académico, se propagó a través de fallas en sendmail y finger, causando una caída del 10 % del Internet de la época. El evento fue

una validación trágica de lo que la comunidad técnica venía advirtiendo por años: que las redes abiertas, mal segmentadas, con *software* compartido y sin controles de autenticación, eran inherentemente inestables (4).

Durante los años 90, las advertencias se transformaron en doctrina. El ejercicio militar *Eligible Receiver* realizado en 1997 —descrito por Warner como un punto de inflexión institucional— demostró que un equipo de ataque usando solo herramientas públicas podía penetrar redes gubernamentales y simular apagones, cortes de comunicación y manipulación de datos (3).

Simultáneamente, comenzaron a consolidarse las amenazas de gran escala vinculadas a motivaciones no técnicas: el espionaje político, el sabotaje económico o la extorsión.

Uno de los episodios más importantes fue el ataque del virus I LOVE YOU (2000). Propagado mediante correo electrónico con un archivo .vbs, infectó millones de sistemas en menos de 24 horas, sobrescribiendo archivos y replicándose a través de las agendas de contactos. No utilizó *exploits* técnicos complejos, sino ingeniería social y el diseño permisivo del sistema operativo Windows. El resultado fue devastador: más de 10.000 millones de dólares en daños, gobiernos paralizados, bancos detenidos y redes corporativas colapsadas (5).

La aparición del *ransomware* WannaCry (2017) marcó un hito: por primera vez, un malware con comportamiento de gusano —basado en un *exploit* desarrollado por la NSA (EternalBlue)— fue utilizado para cifrar datos en más de 200.000 equipos en 150 países, afectando hospitales, sistemas ferroviarios, telecomunicaciones y gobiernos. El *exploit*, filtrado por un actor externo, se apoyaba en una vulnerabilidad ya parcheada por Microsoft; pero no aplicada por miles de instituciones.

El *ramsonware* WannaCry desarrollado a partir de un diseño inseguro, heredado, combinado con sistemas obsoletos e infraestructura crítica interdependiente, dejó en evidencia que la ciberseguridad ya no era un asunto técnico: era una cuestión de continuidad operacional y seguridad nacional (6).

Mucho antes del *software*, la historia de la criptografía ofreció una lección que pareció ignorarse: el caso de Enigma. Diseñada por Alemania para proteger comunicaciones militares, Enigma fue considerada matemáticamente inviolable. Sin embargo, gracias al trabajo de Marian Rejewski, Alan Turing y su equipo en Bletchley Park, fue sistemáticamente rota (7).

El impacto fue decisivo en el desenlace de la Segunda Guerra Mundial. La lección es clara: confiar en la fortaleza matemática o técnica de un sistema, sin prever su modo de falla realista, es un error estratégico. El ecosistema digital heredó esos conceptos: diseñar y desarrollar para el funcionamiento ideal, no para un probable ataque.

6.2. LA CIBERSEGURIDAD COMO CIENCIA DE PREVENCIÓN DE RIESGOS EN ENTORNOS TIC

En un mundo cada vez más digitalizado, la ciberseguridad ha dejado de ser una cuestión técnica reservada a especialistas. Hoy se configura como un elemento esencial para proteger no solo datos o sistemas, sino también la continuidad operativa de organizaciones, la estabilidad de infraestructuras críticas y la confianza en las instituciones.

6.2.1. Definición de la ciberseguridad

La ciberseguridad es el conjunto de estrategias, tecnologías, procesos y políticas diseñadas para proteger los sistemas de información, redes de telecomunicaciones y datos digitales frente a amenazas que comprometen su confidencialidad, integridad, disponibilidad y

autenticidad. En su concepción más amplia, la ciberseguridad constituye una disciplina científica orientada a la gestión y prevención de riesgos en entornos tecnológicos, actuando como un sistema dinámico de protección frente a agresiones intencionadas y no intencionadas en el ciberespacio.

Lejos de ser un concepto estático, la ciberseguridad ha evolucionado desde una visión puramente técnica centrada en firewalls y antivirus, hacia una perspectiva holística que integra factores organizativos, humanos, normativos y económicos. Este enfoque reconoce que los riesgos no solo provienen de actores externos, sino también de vulnerabilidades internas, errores humanos, deficiencias en la configuración de sistemas o fallos estructurales en los procesos organizativos.

Desde una perspectiva científica, la ciberseguridad se fundamenta en el análisis sistemático de riesgos, en la predicción de amenazas emergentes y en la aplicación de metodologías rigurosas para reducir la exposición al riesgo. Así, se alinea con el ciclo de seguridad clásico, en el que se identifican activos, amenazas, vulnerabilidades, y se aplican salvaguardas para mitigar el impacto y la probabilidad de materialización de incidentes.

La ciberseguridad se convierte, por tanto, en un componente esencial de la estrategia organizativa y de la soberanía tecnológica de los Estados, siendo transversal a sectores como la salud, la energía, el transporte, la defensa y las infraestructuras críticas. Su desarrollo implica una constante interacción entre el conocimiento técnico (criptografía, redes, ingeniería inversa), el análisis normativo (*compliance*, regulaciones internacionales) y la gestión estratégica (evaluación de riesgos, políticas de seguridad, gobernanza) (2).

6.2.2. Evaluación de la ciberseguridad

La evaluación de la ciberseguridad es el proceso sistemático mediante el cual se identifican, cuantifican y priorizan los riesgos asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC), con el objetivo de establecer las medidas más eficaces para mitigarlos. Este proceso implica una combinación de metodologías analíticas y herramientas tecnológicas, sustentadas en marcos normativos y buenas prácticas ampliamente aceptadas como ISO/IEC 27001, NIST o MAGERIT, entre otros (2).

A diferencia de una simple auditoría técnica, la evaluación de la ciberseguridad parte del análisis contextualizado de los activos de la organización, entendidos como todo recurso tangible o intangible susceptible de ser atacado, desde infraestructuras físicas y datos, hasta la imagen corporativa o el personal. La identificación y valoración de estos activos constituye el primer paso para delimitar el perfil de exposición al riesgo de una organización.

6.2.2.1. Amenazas

El siguiente componente clave es la identificación de amenazas, que abarca tanto amenazas externas (como ataques cibernéticos dirigidos, malware, espionaje industrial) como internas (errores humanos, malintencionados internos, fallos operativos). Cada amenaza debe analizarse en función del activo al que afecta y del contexto en el que puede materializarse.

6.2.2.2. Vulnerabilidades

En paralelo, se debe evaluar la vulnerabilidad de los activos frente a dichas amenazas, lo cual implica determinar cómo de probable es que una amenaza se materialice con éxito. Esta vulnerabilidad está influida por múltiples factores: deficiencias técnicas, falta de

formación, ausencia de procedimientos, obsolescencia tecnológica, entre otros.

La combinación de estos dos factores —vulnerabilidad e impacto— define el riesgo. El impacto no siempre es cuantificable económicamente; muchas veces es necesario recurrir a escalas cualitativas o a métodos de cuantificación relativa para poder establecer comparaciones y tomar decisiones informadas. Por ejemplo, el impacto de una pérdida de disponibilidad puede expresarse en términos de interrupción de operaciones críticas o afectación a clientes clave.

Una herramienta fundamental en esta fase es la tabla de riesgos, que organiza los riesgos identificados por orden de criticidad. Esta tabla permite a la organización determinar hasta qué punto es rentable asumir o mitigar cada riesgo, introduciendo así el concepto de punto de equilibrio financiero como se presenta en la **figura 6.1**, donde el coste de implementar medidas de seguridad es igual o menor al impacto económico esperado de los riesgos mitigados.

La evaluación de la ciberseguridad no debe concebirse como una actividad puntual, sino como un proceso continuo, iterativo y dinámico. Las organizaciones deben revisar periódicamente sus evaluaciones para adaptarlas a los cambios tecnológicos, a la evolución de las amenazas y a las transformaciones internas. La capacidad de anticipar, detectar y responder de forma ágil a nuevos riesgos es, en última instancia, uno de los pilares de la madurez de una organización (2).

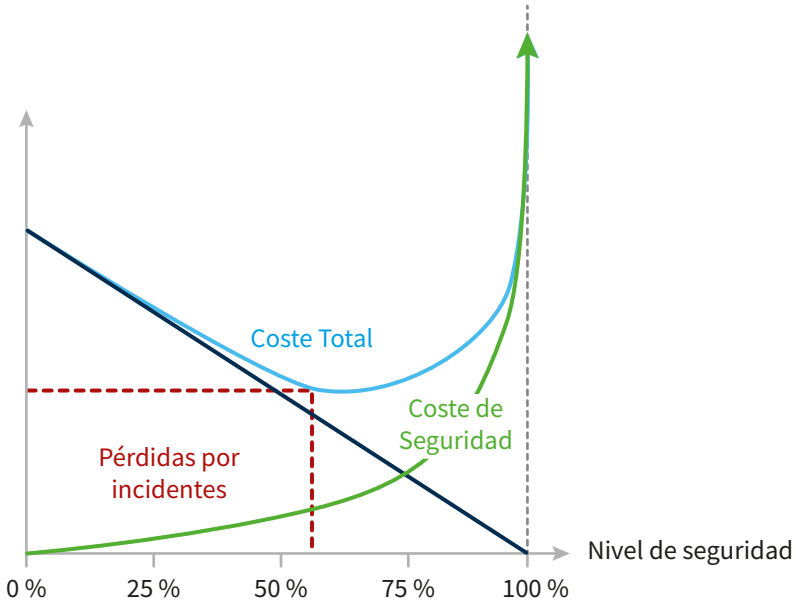


Figura 6.1.
Punto de equilibrio financiero.

6.2.3. Amenazas y tipos de amenazas

Una amenaza en ciberseguridad se define como cualquier circunstancia, evento o agente con el potencial de explotar una vulnerabilidad y causar daño a los activos de una organización. Las amenazas no solo comprometen la integridad, disponibilidad o confidencialidad de los sistemas de información, sino que también pueden poner en riesgo la reputación, la continuidad operativa e incluso la legalidad del funcionamiento institucional.

El estudio y clasificación de las amenazas es una actividad crítica dentro del análisis de riesgos. Para una evaluación efectiva, es necesario agrupar las amenazas según distintos criterios: su origen, el tipo de activo al que afectan y su intencionalidad.

6.2.3.1. Clasificación por origen

6.2.3.1.1. Amenazas de origen natural o ambiental

Estas amenazas no son provocadas por la acción humana e incluyen fenómenos como desastres naturales (inundaciones, terremotos, incendios), fallos en el suministro eléctrico, condiciones climáticas extremas o incluso plagas. Aunque suelen estar fuera del control de la organización, requieren planes de contingencia y medidas de protección física.

6.2.3.1.2. Amenazas humanas (intencionadas y no intencionadas)

Este grupo comprende desde actores externos que intentan comprometer los sistemas hasta el propio personal interno de la organización. Se subdividen en:

- **Externas maliciosas**: ataques dirigidos por ciberdelincuentes, grupos hacktivistas, competidores, o incluso actores estatales. Ejemplos: *malware*, *ransomware*, *phishing*, ataques DDoS, APTs.
- **Internas maliciosas**: empleados con acceso legítimo que abusan de sus privilegios. Este tipo de amenaza es particularmente crítica por su difícil detección.
- **Errores no intencionados del personal**: configuración incorrecta de sistemas, divulgación accidental de información, eliminación involuntaria de datos.

6.2.3.2. Clasificación según el activo objetivo

Cada tipo de activo puede ser objeto de amenazas específicas. A continuación, se describen las más relevantes.

La **tabla 6.1** presenta un esquema de diversas amenazas en el ámbito de la ciberseguridad, clasificadas según el tipo de activo afectado, su

Tabla 6.1. Esquema de clasificación de amenazas.

Activo afectado	Tipo de amenaza	Origen	Impacto principal	Ejemplos
Recursos físicos	Robo, sabotaje, destrucción, fallos ambientales	Natural / Humano externo	Pérdida de disponibilidad y operatividad	Incendio, robo de servidores, corte eléctrico
Utilización de recursos	Uso no autorizado, explotación de servicios, abuso de recursos	Humano interno / externo	Incremento de costos, baja disponibilidad	Instalación de "*dialers*", minería no autorizada
Información almacenada	Acceso indebido, alteración, eliminación	Humano interno / externo	Violación de confidencialidad, integridad y disponibilidad	Acceso no autorizado a bases de datos, malware destructivo
Información en tránsito	Interceptación, modificación, falsificación, repudio	Humano externo	Pérdida de autenticidad, integridad y disponibilidad	Ataque "*man-in-the-middle*", inyección de datos falsos
Imagen y reputación	Difamación, filtraciones, publicidad de fallos de seguridad	Humano externo / interno	Daño reputacional, pérdida de confianza	Publicación de vulnerabilidades en medios, ataques en redes sociales
Daños a terceros	Utilización de recursos como plataforma de ataque	Humano externo (cibercrimen)	Responsabilidad legal y reputacional	Botnets, envío de spam, redireccionamiento de ataques

origen probable, el impacto operativo o estratégico que pueden generar y algunos ejemplos representativos.

Cada fila representa una categoría de activos susceptibles de ser comprometidos dentro de un entorno TIC, desde recursos físicos hasta la reputación institucional. Para cada tipo de activo se identifican las amenazas asociadas, diferenciando su origen (natural, interno, externo, malicioso o no intencionado) y caracterizando el tipo de impacto esperado, que puede incluir la interrupción de operaciones, la pérdida de integridad o confidencialidad de la información, el daño reputacional, o incluso la instrumentalización de los sistemas como plataforma para ataques a terceros.

6.3. DESARROLLO TECNOLÓGICO

Con el avance tecnológico, también han evolucionado las amenazas. Desde los primeros virus informáticos hasta sofisticados ataques de *ransomware*, la ciberseguridad ha tenido que adaptarse constantemente. Además, esta situación ha obligado a las distintas instituciones a actualizar las normativas para incluir estas nuevas situaciones y mantener la seguridad y protección de la sociedad a nivel europeo.

6.3.1. Desarrollo tecnológico y aplicación a la ciberseguridad de tecnologías emergentes en los últimos 20 años

En las últimas dos décadas, el desarrollo tecnológico ha supuesto una transformación en la manera de abordar la seguridad digital. Los últimos avances en tecnología han proporcionado a los ciberatacantes nuevas formas de operar y, por lo tanto, la ciberseguridad desde el punto de vista de la defensa también ha tenido que evolucionar.

En concreto, la inteligencia artificial ha sido uno de los desarrollos clave en los últimos años. Cada vez se encuentra más incorporado en el día a día, habiendo normalizado el uso de asistentes virtuales o modelos avanzados que procesan el lenguaje natural y permiten generar tanto imágenes como voces. Este desarrollo, que ha llegado incluso hasta los primeros prototipos de conducción autónoma, obliga a incrementar la ciberseguridad en ámbitos como el transporte o la protección de nuestros datos, mejorar el análisis de amenazas y los sistemas de detección. Sin embargo, la tecnología es un arma de doble filo, ya que permite también mejorar las defensas, no solo los ataques. En el ámbito de la ciberseguridad, la IA se ha convertido en una herramienta fundamental para detectar actividades maliciosas y responder con rapidez a amenazas emergentes, gracias a su capacidad de aprendizaje y adaptación. Además, la automatización de tareas ha permitido optimizar estas respuestas ante incidentes.

Por otro lado, este periodo de tiempo ha sido testigo del auge del Internet de las Cosas (IoT) y, como consecuencia, ha supuesto un incremento en el tráfico de las redes debido a la mayor interconectividad entre dispositivos. A la vez, el incremento de los dispositivos inteligentes, incluidos los *wearables*, requiere que se definan nuevas estrategias de ciberseguridad para proteger su integridad, ya que amplían la superficie de ataque, dando alternativas a los intrusos para poder acceder a la red o los datos. A esto se le suma la popularización del 5G, que ha revolucionado tanto las redes como la conectividad. Su implementación ha ofrecido conexiones más rápidas, pero también implica nuevos desafíos para la ciberseguridad, que debe proteger las redes de acceso modernas.

Sin ninguna duda, los datos personales están en el punto de mira de las amenazas actuales y la criptografía como medida de protección de la información en tránsito se ha visto gravemente afectada por el desarrollo de la computación cuántica. Este avance puede comprometer los algoritmos de cifrado actuales y dejar al descu-

bierto nuestros datos personales, pero a la vez está impulsando una nueva rama de investigación en criptografía postcuántica que permita garantizar la seguridad de estos datos en el futuro.

En el aspecto económico, las criptomonedas y el *blockchain* han redefinido el concepto de transacciones seguras. Son muy resistentes a la manipulación y proporcionan seguridad en la gestión de los datos, pero esto las convierte en ideales para el uso en actividades fraudulentas y, por lo tanto, requieren una capa de seguridad adicional.

El impacto de estos avances en la sociedad ha sido significativo. Si bien han facilitado el acceso a la información y mejorado la eficiencia en diversos sectores, también han generado nuevos desafíos, como la brecha digital y la pérdida de privacidad. Además, el crecimiento del teletrabajo, especialmente desde la pandemia del COVID-19, y la adopción de servicios en la nube han modificado las estrategias de ciberseguridad, obligando a las organizaciones a implementar medidas adicionales para garantizar la protección de datos en entornos remotos.

La evolución de las ciberamenazas ha acompañado estos avances tecnológicos. A medida que la digitalización se expande, los ataques se han vuelto más sofisticados, exigiendo estrategias de protección más avanzadas y adaptativas.

6.3.2. Las nuevas tecnologías emergentes pretenden ser seguras

En la era digital, tecnologías como la inteligencia artificial, el Internet de las Cosas, el 5G o el *blockchain* han transformado la forma en que se diseñan, desarrollan e implementan los sistemas tecnológicos. Sin embargo, esta evolución no está exenta de riesgos. A medida que se amplía la superficie de ataque y aumentan los niveles de interconectividad, es necesario integrar la seguridad desde las primeras fases del diseño, con métodos que permitan construir sistemas más resistentes y mejor preparados ante fallos o ataques. En este contexto, han surgido herramientas y marcos técnicos clave como los proyectos de OWASP, desarrollados por la comunidad internacional, y los marcos MITRE, impulsados por instituciones públicas, con el objetivo de mejorar la seguridad en los nuevos entornos tecnológicos.

OWASP, *Open Worldwide Application Security Project* (8), es una organización sin ánimo de lucro creada en 2001 que reúne a profesionales de todo el mundo para crear recursos abiertos y prácticos sobre seguridad del software. Uno de sus marcos más conocidos es el *Application Security Verification Standard* (ASVS), que define distintos niveles de verificación —1, 2 y 3—, para comprobar si una aplicación cumple con los requisitos básicos de seguridad según su tipo o nivel de riesgo. Incluye controles técnicos sobre aspectos como autenticación, sesiones, cifrado, validación de datos, gestión de errores o seguridad en el diseño de la arquitectura.

Junto a ASVS, el OWASP Top Ten recopila los diez errores de seguridad más comunes en aplicaciones web. Sirve como guía para desarrolladores, auditores y equipos técnicos, ayudándoles a evitar problemas conocidos como las inyecciones de código, los fallos de control de acceso o la exposición de datos sensibles. Aunque originalmente estaba enfocado en la web tradicional, sus recomendaciones son igualmente útiles en contextos más recientes como IoT, sistemas en la nube o tecnologías *blockchain*, donde los mismos errores se repiten con mayor impacto debido a la complejidad y rapidez del desarrollo.

Con la expansión de la inteligencia artificial, OWASP ha lanzado dos nuevos proyectos: OWASP AI (9) y OWASP GenAI (10). El primero aborda la seguridad de los sistemas que usan aprendizaje automático en todas sus fases: desde la preparación de los datos hasta el uso del modelo en producción. Incluye recomendaciones para proteger los modelos, controlar las inferencias y vigilar el comportamiento del sistema. El segundo se centra en aplicaciones de inteligencia artificial generativa, como los modelos de lenguaje o los generadores de imágenes, y enumera amenazas nuevas como

la manipulación de entradas (*prompt injection*), la filtración de información o la generación de contenidos dañinos. Ambos proyectos proponen controles como validación de entradas y salidas, revisión de comportamiento y registro de actividad para mejorar la confianza en estos sistemas.

Por otro lado, la organización estadounidense MITRE, que trabaja en colaboración con agencias del gobierno, ha desarrollado herramientas muy utilizadas para conocer y enfrentar amenazas reales. MITRE ATT&CK (11) es una base de datos que recoge las tácticas y técnicas que usan los atacantes en entornos reales. Su estructura permite a los equipos de seguridad entender cómo se producen los ataques, en qué fases actúan y qué métodos utilizan. En entornos como IA, IoT o infraestructuras en la nube, ATT&CK ayuda a construir perfiles de ataque realistas y enfocar las defensas en los puntos más débiles del sistema.

Como complemento, MITRE D3FEND ofrece un marco para organizar las defensas. Describe diferentes medidas técnicas que se pueden aplicar para prevenir, detectar, frenar o recuperar ante ataques. Entre ellas se incluyen la segmentación de redes, el control de acceso, la validación de datos, el análisis de comportamiento o la supervisión del tráfico. D3FEND (12) permite conectar cada amenaza con una defensa específica, ayudando a implementar soluciones más prácticas y adaptadas al tipo de sistema que se quiere proteger, ya sea una red 5G, una infraestructura descentralizada o un sistema automatizado.

En conjunto, estos marcos y proyectos muestran cómo el trabajo conjunto entre comunidades técnicas y organismos públicos puede ofrecer herramientas eficaces para construir tecnologías más seguras desde el inicio. Además de mejorar la resistencia técnica de los sistemas, facilitan el cumplimiento de normas como el Reglamento General de Protección de Datos (GDPR) (13), la Directiva NIS2 (14) o las recomendaciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) (15), al ofrecer procesos claros, auditables y adaptados a distintos contextos. La seguridad ya no debe verse como una capa añadida al final del desarrollo, sino como un elemento clave desde el principio. Aunque no exista una tecnología completamente libre de fallos, estos marcos permiten reducir los riesgos y aumentar la confianza en un mundo cada vez más conectado.

6.3.3. Cumplimiento de estándares, recomendaciones y guías de ciberseguridad nacionales, europeas y globales - Interoperabilidad

Los estándares y marcos de ciberseguridad presentados en capítulos anteriores se pueden considerar a nivel global, como la ISO 27001 o el marco de ciberseguridad NIST, ya que son ampliamente utilizados dentro y fuera de la UE, mientras que, en Europa, además son referencias los marcos de ENISA que permiten el cumplimiento de normativas obligatorias como NIS2 o el Reglamento General de Protección de Datos (GDPR).

La normativa ISO requiere una implementación formal que incluya documentación y procesos de auditorías para conseguir certificaciones, a diferencia de otros reglamentos o guías, que tienen mayor flexibilidad y pueden adaptarse a los niveles de madurez de las distintas empresas u organizaciones en materia de ciberseguridad, sin perder el alineamiento con otras regulaciones europeas y proporcionando herramientas para la gestión y evaluación de riesgos.

Cada enfoque tiene sus ventajas y desventajas. Si las organizaciones buscan una certificación reconocida y enfocado a la seguridad de la información, se deben acoger a la normativa ISO 27001, a pesar de su rigidez y el coste de implementación, mientras que, si buscan flexibilidad y adaptabilidad al contexto europeo, las guías de ENISA están alineadas con la regulación de la Unión Europea.

Cada marco tiene su propósito y aplicabilidad según el contexto de la organización. Para empresas en la UE con requerimientos

normativos estrictos, los marcos de ENISA son esenciales, mientras que ISO 27001 es la mejor opción para aquellas que requieren certificaciones. Sin embargo, en ocasiones, el cumplimiento de una normativa no encaja con los requisitos de otras. Por ese motivo, el objetivo de la regulación actual a nivel europeo se encuentra en la búsqueda de la adaptación de los reglamentos obligatorios a la legislación propia de cada Estado miembro.

Uno de los ejemplos más claros es la aplicación del GDPR en distintos países europeos: cada país tiene su propia autoridad supervisora y enfoques específicos, ya que el cumplimiento varía en función de las prioridades nacionales, con algunos países imponiendo sanciones más estrictas que otros. En España se adapta mediante la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), añadiendo a la normativa básica otros derechos como la desconexión digital y está supervisada por la Agencia Española de la Protección de Datos. Alemania o Francia aplican unas de las normativas más estrictas en cuanto a la protección de datos personales, abarcando incluso el ámbito del seguimiento en línea, mientras que en Italia se han impuesto requisitos específicos sobre el tratamiento de datos en el ámbito laboral y sanitario.

Otro caso es el Esquema Nacional de Seguridad (ENS) (16) en España. Es un marco regulatorio para definir los requisitos mínimos de seguridad que deben cumplir obligatoriamente las entidades públicas o las empresas que prestan servicios a la Administración pública, con el objetivo de garantizar una protección adecuada de la información y los servicios digitales. Está regulado por el Real Decreto 311/2022, que adapta los principios a directivas europeas como NIS2 y al Reglamento de Ciberseguridad de la UE.

A pesar de que no existe un Esquema Nacional de Seguridad único a nivel europeo, otros países han desarrollado marcos similares para cumplir con regulaciones europeas: en Alemania, la Oficina Federal de Seguridad de la Información establece un estándar de seguridad de la información (BSI Grundschutz), similar a ISO 27001 pero con mayor enfoque a riesgos específicos.

La interoperabilidad, por tanto, es un tema recurrente y uno de los objetivos de ENISA en la actualidad. Centrándose en la gestión de riesgos de ciberseguridad, la agencia europea está trabajando en un marco único que permita comparar y compartir información sobre evaluaciones de riesgos que utilicen distintos métodos. La necesidad de este esfuerzo surge de que actualmente existen múltiples enfoques tanto a nivel europeo como mundial que no pueden intercambiarse ni comparar sus resultados. Igual que España ha elaborado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), la Agencia de Ciberseguridad Francesa (ANSSI) desarrolló *Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS), que no comparten métodos, nomenclatura ni una escala de riesgos común, por lo que el intercambio de información, como resultados de medidas de mitigación de riesgos entre proyectos con distintas metodologías se convierte en una tarea imposible. Mediante este marco interoperable, ENISA busca traducir cada metodología al estándar definido por la propia agencia (*IT Security Risk Management Methodology*, ITSRM), que considera como base de esta interoperabilidad y que permite establecer comparaciones entre marcos.

6.3.4. La ciberseguridad en Europa: impacto, políticas públicas y normativas

Actualmente, además de impulsar la evolución de políticas y normativas, el impacto económico de las amenazas es significativo: el coste global del cibercrimen en 2020 fue de 5.5 trillones de euros (17), alcanzando en número de incidentes el doble que en 2015. Además, cada vez son amenazas más complejas, aprovechando los últimos avances tecnológicos, como la inteligencia artificial generativa, para evitar ser detectados y afectan a un rango de sectores

cada vez más amplio. Además, los actores involucrados en las amenazas son principalmente grupos vinculados a los Estados, delincuentes con motivaciones financieras, entidades privadas y hacktivistas.

Aproximadamente el 20 % de los ciberataques se enfocan a las administraciones públicas, seguidas del transporte (11 %), entidades financieras e infraestructura digital (9 %), y un 8 % hacia el público general.

Según el *ENISA Threat Landscape* (ETL) (18), que anualmente recoge información sobre los incidentes de ciberseguridad y sus posibles mitigaciones, las principales amenazas y tendencias de los últimos años se enfocan en ocho tipos de amenazas principalmente:

Las amenazas más repetidas afectan a la disponibilidad de servicios o infraestructuras (46 %), donde destaca la denegación de servicio, a pesar de ser incidentes simbólicos y de impacto limitado.

Para seguir, el 27 % de los incidentes en Europa corresponden con ataques de tipo *ransomware*, en los que se toma el control de los activos a cambio de un rescate para liberarlos.

Especialmente relevantes son las amenazas hacia los datos, que abarcan el 16 % de las amenazas. Su importancia radica en el acceso no autorizado de atacantes a datos confidenciales o protegidos, ya que está incluido en el Reglamento General de Protección de Datos (GDPR).

Para tratar de disuadir los ciberataques que amenazan a la Unión Europea, se ha establecido el conjunto de medidas restrictivas (19) que se ha presentado hasta ahora, incluyendo un régimen de sanciones como las multas, inmovilización de activos o prohibición de viajes a cualquier persona implicada en un ciberataque frente a infraestructuras o servicios críticos.

La adopción de normativas como el GDPR, NIS2 o el Reglamento de Ciberresiliencia reflejan el compromiso de establecer ese marco común necesario para garantizar la seguridad de todos los Estados miembros, ya que armoniza requisitos y fortalece la cooperación para enfrentar a las amenazas actuales y emergentes.

6.4. HACIA DÓNDE VAMOS: LÍNEAS FUTURAS EN LA CIBERSEGURIDAD

La historia de la ciberseguridad ha sido, en gran medida, una carrera por alcanzar a la tecnología. Los sistemas que hoy sustentan nuestras comunicaciones, nuestras infraestructuras críticas y buena parte de nuestras vidas digitales fueron concebidos para funcionar, no para resistir. Durante décadas, los avances en conectividad y digitalización han ido muy por delante de las medidas para protegerlos. Hoy, ese desfase ya no es sostenible.

Frente a esta realidad, la pregunta ya no es si habrá ciberataques, sino cuándo y con qué impacto. La ciberseguridad ha dejado de ser una especialización técnica para convertirse en un factor estructural de estabilidad, confianza y resiliencia de nuestras sociedades. Las líneas futuras en este ámbito, por tanto, no se reducen a desarrollos tecnológicos: implican una transformación profunda en cómo pensamos, diseñamos y gobernamos los entornos digitales.

6.4.1. La seguridad como principio de diseño

El primer gran cambio de paradigma es cultural y técnico: la seguridad no puede seguir siendo una capa añadida al final del desarrollo, sino que debe estar presente desde el primer boceto, desde la arquitectura misma del sistema. Esto implica adoptar enfoques como *Security by Design* y *Zero Trust*, que suponen asumir la existencia constante de amenazas, incluso dentro del perímetro interno, y construir defensas desde esa base. Tecnologías

emergentes como la inteligencia artificial, el 5G o el IoT no deben repetir el error de sus predecesores: crecer sin blindarse desde el inicio.

Proyectos como OWASP ASVS, OWASP AI o MITRE D3FEND representan este giro. No se centran solo en cómo responder al ataque, sino en cómo construir infraestructuras que resistan mejor desde el principio. El futuro pasa por sistemas capaces de verificar su comportamiento, auditarse automáticamente y adaptarse a nuevas amenazas sin intervención humana directa.

6.4.2. Gobernanza del riesgo: del técnico al estratégico

Otra transformación clave es la madurez de la gestión del riesgo. Durante mucho tiempo, la ciberseguridad se percibió como un problema de los departamentos de TI. Hoy, es un asunto de gobierno. La protección de los datos, la continuidad operativa, la reputación institucional y el cumplimiento normativo son aspectos que exigen una gobernanza de la ciberseguridad alineada con los objetivos estratégicos de cada organización, sea pública o privada.

En este contexto, la evaluación del riesgo debe ser continua, contextual y multidisciplinar. Debe vincularse a decisiones presupuestarias, a planes de negocio, a políticas públicas. No basta con evaluar amenazas actuales: es necesario anticipar escenarios futuros, incorporar inteligencia sobre actores maliciosos y evaluar la resiliencia institucional ante incidentes de gran escala.

Las normativas europeas como NIS2, DORA o el Reglamento de Cibersolidaridad apuntan en esta dirección. Buscan armonizar criterios, establecer responsabilidades claras y fomentar una respuesta coordinada ante crisis digitales que ya no respetan fronteras ni sectores.

6.4.3. Inteligencia artificial: aliado y amenaza

La inteligencia artificial está llamada a desempeñar un papel protagonista en el futuro de la ciberseguridad. Su capacidad para analizar grandes volúmenes de datos en tiempo real, detectar patrones anómalos y responder de forma autónoma la convierte en una herramienta de defensa clave. Sin embargo, esa misma capacidad puede ser utilizada por actores maliciosos para perfeccionar sus ataques, diseñar amenazas impredecibles o burlar mecanismos de detección tradicionales.

La seguridad de los propios sistemas de IA se vuelve, así, una prioridad. Los modelos generativos, los sistemas de aprendizaje automático y los entornos de inferencia pueden ser manipulados, explotados o utilizados como vectores de ataque. OWASP GenAI ha comenzado a sistematizar estas amenazas y proponer controles, pero aún estamos en una fase inicial.

La línea futura en este ámbito no es solo técnica, sino ética y regulatoria. Requiere definir estándares de transparencia, auditabilidad y responsabilidad en los sistemas autónomos. Requiere garantizar que las decisiones críticas; desde una predicción de fraude hasta una alerta médica, no se basen en modelos opacos, vulnerables o manipulados.

6.4.4. Resiliencia digital en entornos complejos

Las infraestructuras digitales actuales son heterogéneas, interdependientes y, a menudo, opacas. Desde sistemas heredados en organismos públicos hasta redes IoT en hogares, pasando por entornos híbridos en la nube, la superficie de ataque no deja de crecer. En este escenario, pensar en seguridad como prevención total es un error. El objetivo debe ser la resiliencia: la capacidad de resistir, absorber, adaptarse y recuperarse ante incidentes.

Esto implica planes de continuidad robustos, simulaciones de crisis, redundancias estratégicas, formación continua y cooperación público-privada. La resiliencia no es solo tecnológica, es organizativa y humana. Y será uno de los ejes de las políticas públicas en los próximos años, como ya muestran las iniciativas de ENISA o la red EU-CyCLONe.

6.4.5. Soberanía tecnológica y geopolítica de la ciberseguridad

La ciberseguridad ya no es un tema técnico, ni siquiera económico: es geopolítico. Las tensiones internacionales, la dependencia tecnológica, el espionaje industrial y la manipulación de la información digital han convertido el ciberespacio en un nuevo campo de competencia estratégica. Europa ha respondido con una batería normativa ambiciosa, pero enfrenta un reto mayor: reducir su dependencia de tecnologías extranjeras, fortalecer su industria propia y coordinar sus capacidades de defensa digital.

El futuro requiere una soberanía tecnológica real, que no se limite a la infraestructura, sino que incluya estándares, herramientas de auditoría, plataformas de respuesta y formación especializada. Requiere alianzas internacionales, pero también la capacidad de actuar con autonomía. La ciberseguridad, en este marco, será uno de los pilares de la autonomía estratégica europea.

6.5. REFERENCIAS BIBLIOGRÁFICAS

1. Pérez J, Frías Z, Urueña A. La evolución de Internet en España: del Tesys a la economía digital: 50 años de la red de redes [Internet]. Madrid: Red.es; 2018 [citado 31 de marzo de 2025]. Disponible en: https://forohistorico.coit.es/index.php/biblioteca/libros-electronicos/item/50-anos-de-la-red-de-redes-la-evolucion-de-internet-en-espana-del-tesys-a-la-economia-digital

2. Villagrá V. Seguridad en redes de telecomunicación, 1a ed. Cuadernos Cátedra ISDEFE-UPM, no. 5. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones; 2009.

3. Cybersecurity: A Pre-history: Intelligence and National Security [Internet]. 2012 [citado 31 de marzo de 2025];27(5). Disponible en: https://www.tandfonline.com/doi/full/10.1080/02684527.2012.708530?scroll=top&needAccess=tr

4. Orman H. The Morris worm: a fifteen-year perspective [Internet]. IEEE Journals & Magazine. IEEE Xplore. 2003 [citado 31 de marzo de 2025]. Disponible en: https://ieeexplore.ieee.org/abstract/document/1236233

5. Nguyen T. A review of cyber crime, J. Soc. Rev. Dev., vol. 2, n.° 1, Art. n.° 1, ene. 2023.

6. Protection model of PCS of subway from attacks type “wanna cry”, “petya” and “bad rabbit” IoT [Internet]. IEEE Conference Publication. IEEE Xplore; [citado 31 de marzo de 2025]. Disponible en: https://ieeexplore.ieee.org/abstract/document/8317245

7. Singh A, Earle W. Enhancing classical cryptographic systems with modern encryption: a case study on integrating RSA into the enigma machine [Internet]. ICERI2024 Proc. 2024: 8019-8026. DOI: 10.21125/iceri.2024.1957

8. OWASP Foundation. OWASP Top Ten [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://owasp.org/www-project-top-ten/

9. AI Exchange [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://owaspai.org/

10. Owaspllmp, Admin. OWASP Generative AI Security Project, Top 10: LLM & Generative AI Security Risks [Internet]. OWASP Top 10 for LLM & Generative AI Security. [citado 31 de marzo de 2025]. Disponible en: https://genai.owasp.org/

11. MITRE ATT&CK® [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://attack.mitre.org/

12. MITRE D3FEND Knowledge Graph [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://d3fend.mitre.org/

13. GDPR_NEWSurvey.pdf [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://in2mobile.gr/wp-content/uploads/2018/05/GDPR_NEWSurvey.pdf

14. Singh C. The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in By the Network and Information Security 2 (NIS2). Directive 2022/2555. Int. Co Commer Law Rev. 2023 feb; 5:251-261.

15. Home | ENISA [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.enisa.europa.eu/

16. ENS, Esquema Nacional de Seguridad [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://ens.ccn.cni.es/es/

17. Council of the European Union. What are the top cyber threats in the EU? [Internet] Consilium. [citado 31 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/en/policies/top-cyber-threats/#0

18. ENISA. Threat Landscape [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

19. Consilium. Ciberataques: el Consejo prorroga el régimen de sanciones hasta el 18 de mayo de 2025 [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025/

6.6. BIBLIOGRAFÍA

Consejo de la Unión Europea. Cómo refuerza la UE su ciberseguridad [Internet]. Consilium; [citado 31 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/

Ley de Ciberseguridad de la UE | Configurar el futuro digital de Europa [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-act

The Cybersecurity Strategy | Shaping Europe's digital future [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

NIS2 Directive: new rules on cybersecurity of network and information systems | Shaping Europe's digital future [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Páginas - Información Reglamento DORA [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://dgsfp.mineco.gob.es/es/Entidades/Paginas/Informaci%C3%B3n-Reglamento-DORA.aspx

International Organization for Standardization. ISO/IEC 27001:2022 - Information security management systems [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.iso.org/es/norma/27001

Center for Internet Security. CIS Controls [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.cisecurity.org/controls/

ETSI, Standards, mission, vision, direct member participation [Internet]. [citado 31 de marzo de 2025]. Disponible en: https://www.etsi.org/about

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

7

La Regulación Europea del Ecosistema Digital. El Reglamento General de Protección de Datos (RGPD), la Ley de Servicios Digitales (DSA), la Ley de Mercados Digitales (DMA) y la Ley de Inteligencia Artificial

Pilar Rodríguez Pita

Jorge Pérez Martínez

7.1. INTRODUCCIÓN

En los últimos años, la regulación del entorno digital ha experimentado transformaciones profundas, impulsadas por la rápida expansión de las plataformas tecnológicas y los avances en inteligencia artificial. La Década Digital, un concepto clave para la Unión Europea, ha marcado una etapa crucial en la que las tecnologías emergentes y el uso masivo de Internet han redefinido no solo las dinámicas económicas y sociales, sino también las relaciones geopolíticas a nivel global. En este contexto, la UE ha buscado reafirmar su rol como un actor central en la gobernanza digital, en medio de crecientes tensiones entre potencias como Estados Unidos y China, que compiten por alcanzar el liderazgo tecnológico. La necesidad de un entorno regulado y coherente, que no solo proteja a los consumidores, sino que también resguarde principios fundamentales como la privacidad, la transparencia y la equidad, se ha vuelto más urgente que nunca. En este sentido, Europa ha emergido como un referente mundial al poner el foco en la protección de los derechos fundamentales de los usuarios y en la creación de un marco normativo que responda a los desafíos globales, sin perder de vista los valores europeos que han sido clave en su identidad. En la **figura 7.1** se presentan las principales iniciativas legislativas dentro de la Década Digital europea.

A lo largo de este capítulo se evaluará el marco regulatorio europeo en dos etapas clave: la regulación previa a la llamada Década Digital, que incluyó instrumentos fundamentales como el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre Comercio Electrónico, y las nuevas normativas surgidas en este período reciente, como el Digital Services Act (DSA), el Digital Markets Act (DMA), la Artificial Intelligence Act (AI Act) y el Chips Act, entre otros.

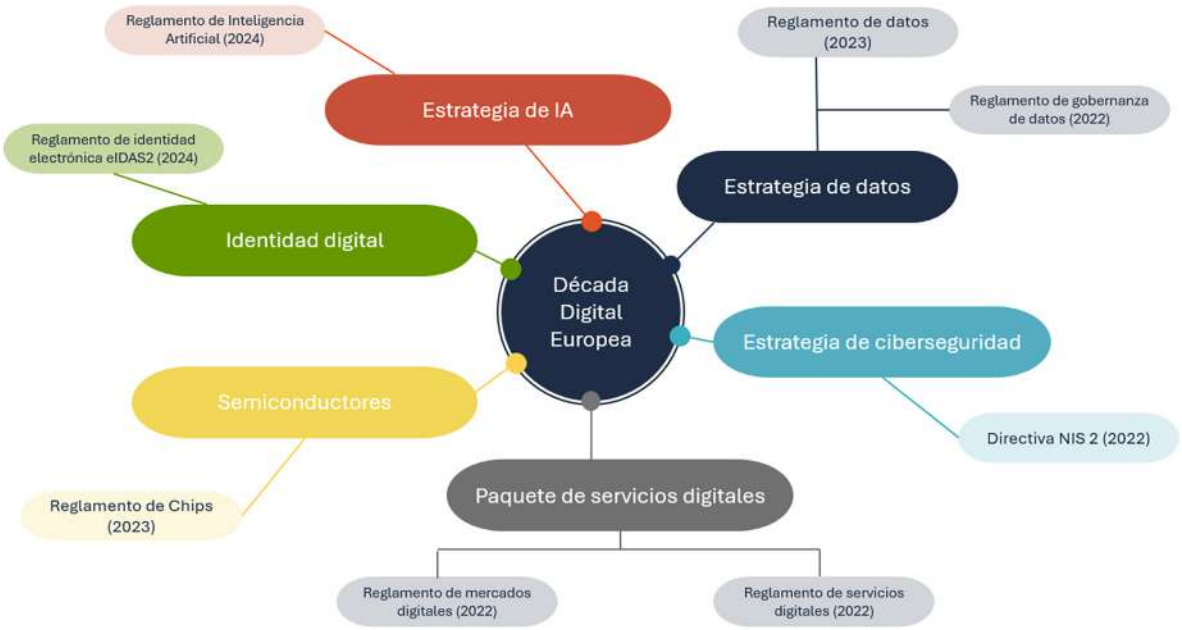


Figura 7.1.
Legislación aprobada en la Década Digital europea.

7.2. UNA MIRADA HACIA ATRÁS

Antes de la llegada de la Década Digital, la Unión Europea ya había dado pasos significativos para regular el entorno digital, sentando las bases de un mercado más seguro, transparente y equitativo. Normativas como la Directiva sobre Comercio Electrónico y el Reglamento General de Protección de Datos (RGPD) marcaron hitos clave al definir derechos y obligaciones en un ecosistema en constante evolución. Estas regulaciones no solo impulsaron la confianza en el comercio en línea y la protección de los datos personales, sino que también establecieron un marco común para los Estados miembros. Sin embargo, a medida que las plataformas digitales crecían en alcance e influencia, se hizo evidente la necesidad de actualizar y reforzar estas reglas para responder a los nuevos desafíos de la era digital.

7.2.1. El Reglamento General de Protección de datos

El Reglamento General de Protección de Datos (RGPD) es la normativa más estricta a nivel mundial en materia de privacidad y seguridad de datos. Adoptado en 2016 y en vigor desde el 25 de mayo de 2018, tiene como objetivo reforzar los derechos fundamentales de los ciudadanos en la era digital y armonizar la legislación en todos los Estados miembros de la Unión Europea (1). Sustituyendo la Directiva de Protección de Datos de 1995, el RGPD establece un marco unificado que reduce la fragmentación normativa y la carga administrativa para empresas y organismos públicos.

El RGPD se basa en siete principios esenciales para el tratamiento de datos personales (2):

1. Licitud, lealtad y transparencia: los datos deben procesarse de forma justa y transparente.
2. Limitación de la finalidad: solo pueden utilizarse para los fines legítimos expresamente indicados.
3. Minimización de datos: se debe recoger únicamente la información estrictamente necesaria.
4. Exactitud: los datos deben ser precisos y estar actualizados.
5. Limitación del almacenamiento: no pueden conservarse más tiempo del necesario.
6. Integridad y confidencialidad: se deben aplicar medidas de seguridad adecuadas.
7. Responsabilidad proactiva: los responsables del tratamiento deben demostrar el cumplimiento del RGPD.

Además, el RGPD otorga a los ciudadanos un mayor control sobre su información personal mediante derechos específicos, como el derecho de acceso y portabilidad, que permite a los interesados obtener sus datos en un formato estructurado y de uso común, facilitando su transferencia a otro proveedor sin impedimentos técnicos ni costos adicionales. El derecho de rectificación y supresión les ofrece la posibilidad de corregir información errónea o desactualizada, así como solicitar la eliminación de sus datos en determinadas circunstancias, como cuando estos ya no sean necesarios para los fines con los que fueron recopilados o cuando el interesado retire su consentimiento. También se reconoce el derecho de oposición y restricción del tratamiento, permitiendo a los ciudadanos rechazar el uso de sus datos en ciertos contextos, como el marketing directo, o solicitar una limitación temporal del procesamiento mientras se resuelven disputas sobre su exactitud o legalidad. Asimismo, el derecho a la transparencia y consentimiento explícito garantiza que el uso de datos personales solo puede basarse en una autorización clara e informada, evitando prácticas engañosas o confusas en la obtención del consentimiento. Este principio se traduce en la exigencia de formularios y políticas de privacidad comprensibles, sin tecnicismos, con opciones de aceptación activa en lugar de casillas premarcadas o términos ambiguos.

El reglamento también impone obligaciones tanto a los responsables del tratamiento, que determinan cómo y por qué se usan los datos, como a los encargados del tratamiento, que

procesan la información en su nombre. Ambos deben aplicar medidas de seguridad adecuadas al nivel de riesgo, como la seudonimización o el cifrado de datos, así como la implementación de mecanismos de prevención ante accesos no autorizados. Además, están obligados a notificar violaciones de seguridad a la autoridad de control en un plazo máximo de 72 horas desde que tengan conocimiento del incidente, proporcionando detalles sobre su naturaleza, el impacto potencial y las acciones correctivas implementadas. En los casos en que una brecha de seguridad represente un alto riesgo para los derechos y libertades de los afectados, también deben informar a los propios interesados sin demoras injustificadas. Para garantizar una gestión adecuada de la privacidad, algunas organizaciones, especialmente aquellas que manejan grandes volúmenes de datos sensibles o realizan monitoreos sistemáticos a gran escala, deben nombrar un Delegado de Protección de Datos (DPD). Esta figura, independiente dentro de la organización, es responsable de supervisar el cumplimiento normativo, asesorar sobre las mejores prácticas y actuar como punto de contacto con las autoridades de supervisión y los ciudadanos.

Asimismo, para facilitar el cumplimiento en empresas con operaciones en varios Estados miembros, el RGPD establece el mecanismo de ventanilla única, lo que significa que las organizaciones solo tienen que tratar con una única autoridad de control en el país donde tengan su establecimiento principal, evitando la complejidad de múltiples regulaciones nacionales y facilitando la gestión del cumplimiento a nivel transfronterizo.

La supervisión y aplicación del RGPD están a cargo del Comité Europeo de Protección de Datos (EDPB), organismo que coordina la interpretación y aplicación uniforme del reglamento en toda la Unión Europea, asegurando que no existan discrepancias entre los Estados miembros (3). Para ello, el EDPB emite directrices y recomendaciones sobre aspectos clave de la normativa, además de resolver disputas entre autoridades nacionales cuando surgen divergencias en la toma de decisiones.

Cada país debe contar con una autoridad nacional de protección de datos, encargada de supervisar el cumplimiento de la normativa, investigar posibles infracciones y gestionar las reclamaciones de los ciudadanos. Estas autoridades tienen potestad para llevar a cabo auditorías, imponer medidas correctivas y, en caso de incumplimiento, aplicar sanciones (4).

Las multas por violaciones al RGPD son proporcionales a la gravedad de la infracción y pueden alcanzar hasta 20 millones de euros o el 4 % del volumen de negocios anual global de la empresa infractora, lo que supone un incentivo significativo para que las organizaciones implementen medidas sólidas de cumplimiento. Además de las multas económicas, las autoridades pueden imponer restricciones sobre el tratamiento de datos, suspender flujos de información internacional e incluso prohibir ciertas prácticas que no se ajusten a la normativa.

A lo largo de los años, el RGPD ha demostrado su efectividad en la aplicación de sanciones significativas contra grandes corporaciones tecnológicas, reforzando su papel como un estándar global de referencia en la protección de datos personales. En particular cabe destacar el caso Google (5), en el que, en 2019, la CNIL, autoridad francesa de protección de datos, impuso a Google una multa de 50 millones de euros por incumplir el RGPD, específicamente por falta de transparencia en el tratamiento de datos personales y por no obtener un consentimiento válido para la personalización de anuncios. Se identificó que la información proporcionada a los usuarios era difícil de entender y estaba dispersa en múltiples documentos, lo que dificultaba la comprensión sobre el uso de sus datos. Además, el consentimiento para la publicidad personalizada no cumplía con los requisitos del reglamento, ya que no era específico ni suficientemente informado, y en algunos casos, las casillas de aceptación estaban premarcadas. Esta sanción marcó un precedente en la aplicación del RGPD, destacando la necesidad de garantizar transparencia y un control real de los usuarios sobre su información personal. Como consecuencia, Google modificó sus políticas de privacidad y consentimiento para ajustarse a la normativa, y

el caso incentivó a otras empresas a revisar sus prácticas para evitar sanciones similares, contribuyendo a una mayor concienciación sobre los derechos digitales y la protección de datos.

Otro caso con gran repercusión también fue el de Meta en 2023 (6), que fue sancionada con una multa récord de 1.200 millones de euros por infringir el RGPD al transferir datos de usuarios europeos a servidores en Estados Unidos sin garantizar un nivel adecuado de protección, lo que suponía una violación de las disposiciones sobre transferencias internacionales de datos. Se determinó que la empresa no había implementado medidas suficientes para salvaguardar la seguridad y privacidad de la información transferida, lo que llevó a reforzar la importancia del cumplimiento de las normativas en este ámbito. Esta sanción no solo subrayó la necesidad de proteger la privacidad de los usuarios, sino que también ejerció presión sobre otras compañías para que garantizaran la seguridad de los datos en un contexto global. Como consecuencia, Meta tuvo que revisar sus políticas y buscar soluciones para ajustarse al RGPD, mientras que el caso generó un debate sobre la necesidad de acuerdos internacionales más sólidos para proteger la información personal en un entorno global.

Finalmente, el RGPD también regula las transferencias internacionales de datos, exigiendo que los países receptores garanticen un nivel de protección adecuado. La Comisión Europea evalúa estos niveles mediante decisiones de adecuación y, en ausencia de ellas, las transferencias pueden realizarse bajo cláusulas contractuales tipo u otras garantías específicas.

7.2.2. La Directiva de comercio electrónico

La Directiva sobre el Comercio Electrónico (7) establece un marco armonizado para regular los servicios en línea en la Unión Europea, garantizando la transparencia, la protección del consumidor y la responsabilidad de los proveedores. Entre sus disposiciones clave se incluyen requisitos de información para los prestadores de servicios, normas sobre comunicaciones comerciales y contratos electrónicos, así como la limitación de responsabilidad para los intermediarios. Asimismo, fomenta la cooperación administrativa entre los Estados miembros y promueve mecanismos de autorregulación.

Uno de los principios fundamentales de la Directiva es la denominada "cláusula del mercado interior", que establece que los proveedores de servicios en línea están sujetos únicamente a la legislación del Estado miembro en el que están establecidos, evitando la aplicación de normativas divergentes en los distintos países donde sus servicios son accesibles (8). Esto refuerza la seguridad jurídica y facilita la expansión del comercio digital en la UE.

En cuanto a la responsabilidad de los intermediarios, la Directiva estipula que estos no son responsables de los contenidos ilícitos que alojan si cumplen con determinadas condiciones, como la eliminación rápida del contenido ilegal una vez detectado. Sin embargo, no se les puede imponer una obligación general de supervisión, lo que protege su función neutral y meramente técnica en la gestión de la información.

La regulación abarca un amplio espectro de servicios digitales, desde la venta en línea de productos y servicios hasta la publicidad digital, los servicios profesionales, de entretenimiento e intermediación. Su alcance se extiende a cualquier servicio prestado a distancia mediante medios electrónicos a solicitud de un usuario, lo que la convierte en la base regulatoria del ecosistema digital europeo.

Desde su adopción en el año 2000, la Directiva ha sido objeto de interpretaciones y aclaraciones por parte del Tribunal de Justicia de la UE, especialmente en lo relativo al principio de país de origen y a la exención de responsabilidad de los intermediarios. No obstante, persisten divergencias entre los Estados miembros respecto a la aplicación de estas normas, lo que ha impulsado la introducción de nuevas reglas y mecanismos de aplicación para abordar desafíos emergentes, como la desinformación en línea, los contenidos ilícitos y el pago de derechos de autor por parte de plataformas de intercambio de contenido (9).

7.3. UNA EUROPA ADAPTADA A LA ERA DIGITAL

En 2019, con la renovación de la Comisión Europea, la adaptación de Europa a la Era Digital se consolidó como una de las prioridades estratégicas de la nueva agenda política, con el objetivo de garantizar una transformación digital equitativa, segura y alineada con los valores europeos (10). Para ello, la Comisión promovió un marco normativo integral que abordara los desafíos del entorno digital, estableciendo regulaciones en materia de servicios digitales, competencia en mercados digitales, protección de datos, ciberseguridad e inteligencia artificial. Estas iniciativas incluyeron la supervisión de grandes plataformas en línea, la regulación del uso de la inteligencia artificial bajo principios éticos, el fortalecimiento de la gobernanza de datos y el desarrollo de infraestructuras digitales resilientes. Además, se impulsaron inversiones en innovación y programas de digitalización para la industria, la administración pública y la educación, con el fin de fortalecer la competitividad europea en la economía digital global. Así, la estrategia de la Comisión no solo buscaba fomentar el avance tecnológico, sino también asegurar que este se desarrollara en un marco regulador que protegiera los derechos de los ciudadanos y garantizara una competencia justa en el ecosistema digital.

7.3.1. La Ley de Servicios Digitales

El Reglamento (UE) 2022/2065 tiene como propósito regular la actividad de los intermediarios y plataformas en línea, incluyendo mercados digitales, redes sociales, plataformas de intercambio de contenidos, tiendas de aplicaciones, y servicios de viaje y alojamiento en línea. Su objetivo principal es prevenir actividades ilícitas y perjudiciales en el entorno digital, así como frenar la propagación de la desinformación (11).

Esta normativa se erige como la primera legislación a nivel mundial que exige a las empresas de servicios digitales en la Unión Europea asumir responsabilidades sobre los contenidos publicados en sus plataformas (12). En este sentido, el Reglamento de Servicios Digitales establece una serie de obligaciones específicas para los proveedores de servicios digitales, entre las cuales se incluyen nuevas medidas para la detección, eliminación y mitigación de contenidos ilegales en línea, con requisitos específicos que obligan a las plataformas a actuar de manera rápida y eficaz ante la identificación de publicaciones que infrinjan la normativa. Además, se han endurecido los criterios de trazabilidad y los mecanismos de control aplicables a los comercios en línea, con el objetivo de garantizar una mayor supervisión de las actividades comerciales y prevenir el fraude. En paralelo, se han reforzado las exigencias de transparencia y rendición de cuentas por parte de las plataformas digitales, especialmente en lo que respecta a sus sistemas de recomendación de contenidos y a la publicidad personalizada, regulando de manera más estricta la recopilación y el uso de datos personales de los usuarios. Asimismo, la normativa prohíbe expresamente ciertas prácticas engañosas, como la manipulación algorítmica orientada a inducir decisiones de consumo involuntarias, así como determinadas formas de publicidad selectiva que puedan resultar invasivas o discriminatorias (13).

Asimismo, el reglamento introduce condiciones específicas para las grandes plataformas en línea (14). Hasta la fecha, la Comisión ha identificado 23 plataformas en línea de muy gran tamaño, así como dos motores de búsqueda de gran alcance (15).

El incumplimiento de estas disposiciones conlleva sanciones proporcionales al tamaño de las empresas afectadas. En el caso de aquellas con menos de 45 millones de usuarios activos, estarán sujetas a las sanciones establecidas en la legislación nacional de cada Estado miembro, incluyendo posibles multas. Por su parte, las empresas que superen esta cifra podrán enfrentarse a multas de hasta el 6 % de su volumen de negocios mundial (15).

7.3.2. La Ley de Mercados Digitales

La Ley de Mercados Digitales (DMA, por sus siglas en inglés) es un marco regulador adoptado por la Unión Europea para garantizar la competencia justa en los mercados digitales y prevenir abusos de poder por parte de las grandes plataformas tecnológicas. Su objetivo principal es doble: por un lado, asegurar que los mercados en los que operan estas plataformas sigan siendo competitivos, permitiendo que otros actores puedan desafiar su posición; y por otro, garantizar la equidad, estableciendo un entorno de igualdad de condiciones para empresas y consumidores en el mercado digital de la UE. Para ello, la Comisión Europea presentó esta propuesta basándose en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), con el fin de evitar divergencias normativas que obstaculicen la prestación transfronteriza de servicios digitales y asegurar un marco regulador uniforme dentro del mercado único (16).

Para lograr estos objetivos, la DMA introduce un enfoque *ex ante*, es decir, establece reglas preventivas para regular la actuación de las grandes plataformas antes de que se produzcan abusos de poder. Esto representa un cambio significativo respecto a las normativas de competencia tradicionales de la UE, que actúan *ex post*, es decir, después de que se haya producido una infracción. La DMA complementa, pero no modifica, las normas de competencia existentes y busca armonizar las reglas del mercado digital en toda la Unión (17).

Un aspecto clave de la DMA es la designación de guardianes de acceso, que son grandes plataformas digitales que prestan servicios esenciales como motores de búsqueda, tiendas de aplicaciones y servicios de mensajería. Estos guardianes de acceso estarán sujetos a una serie de obligaciones y prohibiciones específicas para limitar su poder y fomentar la competencia (18).

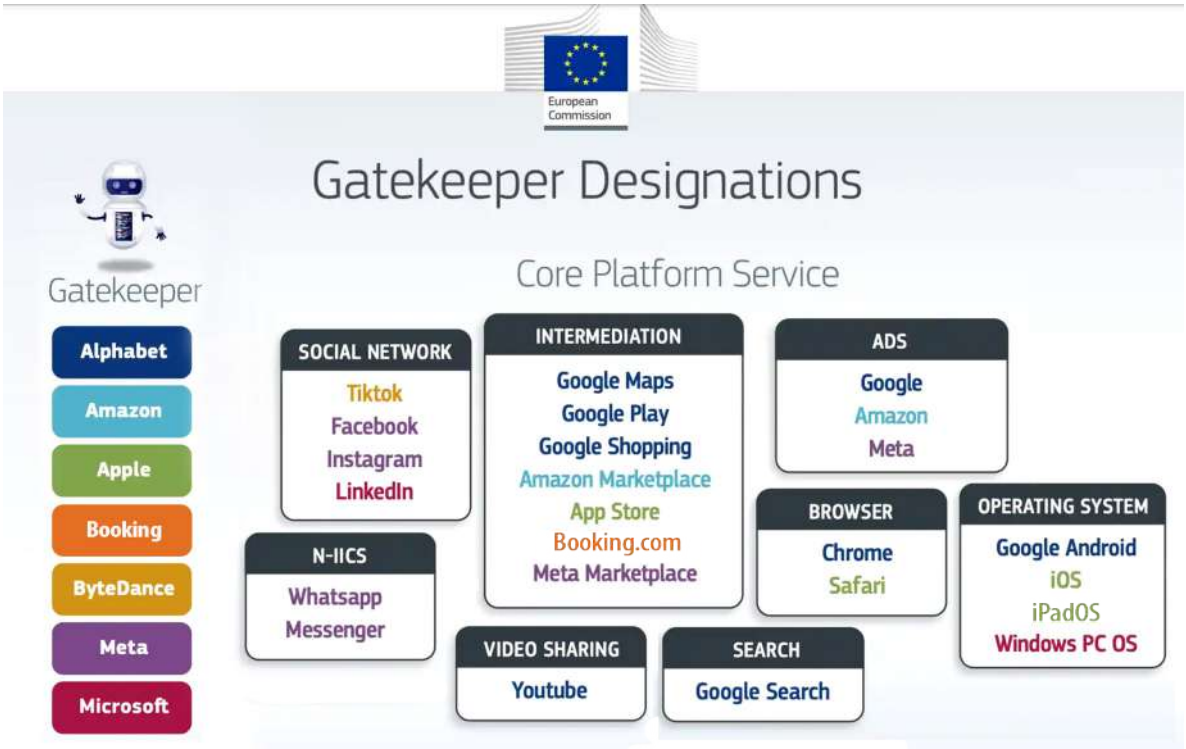


Figura 7.2.
Guardianes de acceso de acuerdo con la ley de mercados digitales (20).

La Comisión Europea propuso inicialmente esta regulación en diciembre de 2020, y tras su aprobación por el Parlamento Europeo y el Consejo el 14 de septiembre de 2022, la norma fue publicada en el Diario Oficial el 12 de octubre de 2022. Entró en vigor el 1 de noviembre de 2022 y comenzó a aplicarse el 2 de mayo de 2023 (19).

El 6 de septiembre de 2023, la Comisión Europea designó por primera vez a seis guardianes de acceso en el marco de la DMA. Las empresas identificadas fueron Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft. Posteriormente, el 29 de abril de 2024, la Comisión amplió esta clasificación al incluir a Apple en relación con su sistema operativo para tabletas, iPadOS. Asimismo, el 13 de mayo de 2024, la plataforma Booking.com fue designada como guardián de acceso debido a su papel en los servicios de intermediación en línea. En total, la Comisión ha designado 24 servicios básicos de plataforma proporcionados por estas empresas, que dispondrán de un plazo máximo de seis meses para garantizar el cumplimiento de sus nuevas obligaciones bajo la supervisión de la Comisión Europea (20). En la **figura 7.2** se puede encontrar una referencia de las plataformas y sus servicios identificados.

7.3.3. La identidad digital europea

El marco de identidad digital europea ha sido objeto de una actualización con el fin de mejorar el acceso de los ciudadanos a los servicios digitales y reforzar el control sobre su información personal. La Regulación eIDAS (21) estableció el primer marco transfronterizo para identidades digitales de confianza y servicios electrónicos, permitiendo interacciones seguras entre ciudadanos, empresas y administraciones públicas. Su objetivo era facilitar el acceso de los ciudadanos a los servicios públicos en toda la UE mediante un sistema de identificación electrónica reconocido mutuamente por los Estados miembros. Sin embargo, una evaluación de la Comisión Europea concluyó que la normativa solo había cumplido parcialmente sus objetivos, debido a su estructura, su implementación limitada y la evolución del entorno tecnológico y las expectativas de los usuarios (22).

En respuesta a estos desafíos, la presidenta de la Comisión Europea, Ursula Von der Leyen, anunció en su discurso sobre el Estado de la Unión del 16 de septiembre de 2020 una iniciativa para desarrollar una identidad digital europea (23). Esta propuesta tenía como propósito simplificar el acceso a los servicios digitales en Europa y garantizar a los ciudadanos un mayor control sobre los datos que desean compartir. Como parte de esta estrategia, el 3 de junio de 2021, la Comisión Europea presentó una propuesta de reglamento para actualizar el marco de identidad digital europea, introduciendo como principal innovación la cartera de identidad digital europea.

Esta actualización responde a los objetivos fijados en la estrategia digital de la UE, recogida en el Brújula Digital 2030, que establece que, para finales de la década, todos los servicios públicos clave deberán estar disponibles en línea, y todos los ciudadanos deberán tener acceso a su historial médico digital y a una identificación digital (24). Además, la Comisión espera que el nuevo marco de identidad digital ofrezca mayores garantías de seguridad y control, permitiendo a los ciudadanos gestionar quién tiene acceso a su identidad digital y qué datos pueden ser compartidos (25).

7.3.4. El reglamento europeo de chips

La Ley Europea de Chips es una iniciativa clave de la Unión Europea para fortalecer su competitividad y resiliencia en el sector de los semiconductores, un elemento fundamental en la transición digital y ecológica. Su objetivo es abordar la escasez de *chips*, reforzar el liderazgo tecnológico europeo y movilizar más de 43.000 millones de euros en inversiones públicas y privadas (26). Además, busca establecer un marco de preparación y respuesta ante futuras

crisis de suministro, en colaboración con los Estados miembros y socios internacionales.

El sector de los semiconductores es altamente estratégico, ya que constituye la base de la transición digital. Sin embargo, su producción depende de cadenas de suministro globales complejas y vulnerables. Actualmente, la capacidad de fabricación de Europa representa menos del 10 % del total mundial y en tecnologías avanzadas (procesos de 7 y 5 nanómetros), la producción se concentra completamente en Asia, con Taiwán y Corea del Sur dominando el mercado. La dependencia de estos actores representa un desafío para la seguridad económica y tecnológica de la UE (27).

En este contexto, la Comisión Europea presentó en febrero de 2022 una propuesta para la Ley Europea de Chips, basada en tres pilares fundamentales que han sido mantenidos por los colegisladores (28):

- Fomento de la innovación: la iniciativa Chips para Europa impulsará el desarrollo de capacidades tecnológicas y la innovación a gran escala dentro del ecosistema europeo de semiconductores.
- Seguridad del suministro: se establecerá un marco de incentivos para atraer inversiones en infraestructuras de producción dentro de la UE, con el objetivo de garantizar un suministro estable y reducir la dependencia de terceros países.
- Mecanismo de respuesta a crisis: se creará un Consejo Europeo de Semiconductores que coordinará a la Comisión, los Estados miembros y las partes interesadas. Además, en caso de crisis de suministro, la Comisión podrá aplicar medidas de emergencia, como solicitar información a las empresas, priorizar pedidos críticos o realizar compras conjuntas en nombre de los Estados miembros.

La presidenta de la Comisión, Ursula Von der Leyen, presentó esta estrategia en su discurso sobre el Estado de la Unión de 2021, con el objetivo de crear un ecosistema europeo de chips de vanguardia que abarque producción, investigación, diseño y pruebas (29). En 2022, destacó la inminente apertura de la primera gigafábrica de chips en Europa, como parte de esta iniciativa (30).

El Parlamento Europeo y el Consejo aprobaron la Ley Europea de Chips el 18 de abril de 2023, tras 14 meses de negociaciones y cuatro rondas de diálogo interinstitucional. Posteriormente, el Parlamento adoptó su posición en julio de 2023, y la normativa entró en vigor el 21 de septiembre de 2023.

Históricamente, la UE ha intentado reducir su dependencia en este sector. En 2013, la Comisión adoptó una estrategia para micro y nanoelectrónica con el objetivo de revertir la disminución de la cuota europea en el mercado global (31). Sin embargo, la propia Comisión reconoció que no logró sus objetivos (32). Actualmente, Europa mantiene una posición sólida en ciertos segmentos, como propiedad intelectual y herramientas de fabricación, pero presenta debilidades en diseño, automatización y ensamblaje, sectores dominados por empresas estadounidenses y asiáticas.

El sector de los semiconductores es también un motor clave para el empleo en la UE. En 2018, aproximadamente 219.000 personas trabajaban en la fabricación de componentes electrónicos, con un crecimiento anual del 3 % entre 2012 y 2018. En total, la microelectrónica europea emplea directamente a 455.000 profesionales altamente cualificados y, como sector habilitador para toda la cadena de valor de la electrónica, genera alrededor de 2,6 millones de empleos en total, con un impacto multiplicador de 5,7 empleos adicionales por cada trabajador del sector (33).

7.3.5. La Estrategia Europea de Datos

La Estrategia Europea de Datos, presentada por la Comisión Europea en la (34), tiene como objetivo consolidar a la Unión Europea como un actor líder en la economía digital mediante el desarrollo de un mercado único de datos. Este marco regulador busca garantizar la libre circulación de datos entre Estados miembros y sectores económicos, respetando los principios

de privacidad, protección de datos y competencia leal.

La estrategia se articula en torno a varios ejes fundamentales. En primer lugar, promueve el empoderamiento de los ciudadanos, otorgándoles mayor control sobre sus datos personales y facilitando el acceso a servicios innovadores. Asimismo, fomenta el desarrollo tecnológico y la innovación, impulsando la reutilización de datos no personales e industriales en ámbitos estratégicos como la salud, la movilidad y la sostenibilidad ambiental. Otro aspecto central de la estrategia es la inversión en infraestructuras avanzadas para el almacenamiento y procesamiento de datos, así como el establecimiento de un marco normativo que garantice el acceso equitativo y seguro a la información. Además, prevé la creación de espacios de datos sectoriales interoperables en áreas clave como la sanidad, la energía y la agricultura, con el fin de optimizar el uso de la información en beneficio del desarrollo económico y social. Finalmente, la Estrategia Europea de Datos se alinea con los compromisos del Pacto Verde Europeo (35), promoviendo el uso de datos como herramienta para fortalecer la sostenibilidad y facilitar la transición ecológica en la Unión.

Se han desarrollado tres principales iniciativas legislativas recogidas en la **figura 7.3**:

Figura 7.3.
Instrumentos legales desde la perspectiva del tipo de datos.
Elaboración propia a partir de (36).

7.3.5.1. Reglamento de Gobernanza de Datos

El Reglamento de Gobernanza de Datos (*Data Governance Act* o DGA) es una pieza clave dentro del marco normativo de la Unión Europea, cuyo objetivo es establecer un ecosistema de datos que impulse la transformación digital de los Estados miembros y contribuya a los objetivos de la Década Digital Europea. Su ámbito de aplicación abarca tanto datos personales como no personales, garantizando la coherencia con el Reglamento General de Protección de Datos (RGPD) y estableciendo salvaguardias que fomentan la confianza en la reutilización de datos (37).

El DGA regula la reutilización de datos protegidos de titularidad pública, como datos personales o comerciales sujetos a derechos de terceros, y promueve el intercambio de datos mediante la regulación de intermediarios especializados. Asimismo, incentiva el uso altruista de datos con fines de interés público y establece el Comité Europeo de Innovación en

Materia de Datos para facilitar la cooperación y el intercambio de mejores prácticas entre los Estados miembros (38).

En la práctica, el reglamento impone requisitos técnicos a las administraciones públicas para garantizar la privacidad y confidencialidad en la reutilización de datos, mediante herramientas como la anonimización, la seudonimización o entornos de tratamiento seguro. Además, introduce normas sobre accesibilidad y tarifas, limitando los acuerdos exclusivos de reutilización y estableciendo tasas proporcionales al coste del servicio, con incentivos específicos para la investigación científica y las pymes. Para agilizar los procesos, los organismos del sector público deben resolver las solicitudes en un plazo máximo de dos meses y contar con el apoyo de entidades especializadas (39).

Para mejorar la transparencia y accesibilidad, los Estados miembros deben crear un punto único de información sobre los datos disponibles, complementado a nivel europeo por el Registro Europeo de Datos Protegidos en Posesión del Sector Público (ERPD), facilitando así la reutilización de datos tanto dentro del mercado interior como a nivel internacional.

7.3.5.2. Reglamento de datos

El Reglamento de Datos (40) es un marco legislativo diseñado para fortalecer la economía digital de la UE mediante la promoción de un mercado de datos equitativo y competitivo. Su objetivo principal es mejorar el acceso y la utilización de datos, en particular los datos industriales, con el fin de fomentar la innovación y garantizar una distribución justa del valor generado en la economía de los datos. La normativa establece con claridad quién puede acceder a qué datos y bajo qué condiciones, asegurando un equilibrio entre la protección de derechos y la promoción de la reutilización de datos. La propuesta parte de la premisa de que el derecho de uso de los datos no personales posee un valor intrínseco y que dicho valor debe distribuirse de manera equitativa entre los distintos actores económicos (41). En este sentido, la Ley de Datos busca facilitar el acceso y uso de datos por parte de consumidores y empresas, garantizando seguridad jurídica en la compartición de datos dentro de la UE, permitir el uso de datos por parte de organismos públicos en situaciones excepcionales donde exista una necesidad urgente de datos, favorecer la interoperabilidad y la portabilidad de datos asegurando la posibilidad de cambio entre servicios de computación en la nube y en el borde, proteger contra transferencias ilegales de datos estableciendo salvaguardas específicas para proveedores de servicios en la nube y desarrollar estándares de interoperabilidad que permitan la reutilización de datos en distintos sectores económicos (42).

El marco armonizado de la normativa establece que los usuarios de un producto o servicio puedan acceder a los datos generados durante su uso. Los fabricantes y proveedores de servicios estarán obligados a diseñar productos que permitan la accesibilidad a los datos de forma predeterminada y deberán garantizar transparencia respecto a qué datos estarán disponibles y cómo podrán ser consultados. En los casos en que el acceso directo no sea posible, los titulares de los datos deberán proporcionarlos sin demoras injustificadas, sin coste adicional y, cuando sea posible, en tiempo real. Asimismo, la Ley de Datos introduce un derecho ampliado de portabilidad, que va más allá del establecido en el Artículo 20 del Reglamento General de Protección de Datos (RGPD). Este derecho otorga a usuarios y empresas la facultad de compartir tanto datos personales como no personales con terceros, siempre que así lo soliciten. Sin embargo, los proveedores designados como "guardianes de acceso" (*gatekeepers*) bajo la Ley de Mercados Digitales (DMA) no podrán acceder a estos datos, con el fin de evitar prácticas anticompetitivas.

La normativa también establece una serie de obligaciones para los titulares de datos, quienes deberán proporcionar acceso bajo términos justos, razonables, no discriminatorios y transparentes. Se prohíbe la discriminación entre diferentes tipos de receptores de datos y la concesión de derechos exclusivos, salvo que el usuario así lo solicite. Los titulares de datos

podrán recibir compensación por facilitar el acceso a datos, pero esta deberá ser razonable y proporcional a los costes incurridos. En el caso de pequeñas y medianas empresas (PYMEs), cualquier compensación no podrá superar los costos de provisión de datos, salvo que normativas sectoriales indiquen lo contrario. Para evitar abusos en el uso de datos, la normativa prohíbe que los receptores de datos los utilicen para desarrollar productos que compitan directamente con los de la empresa que originó los datos. Asimismo, la información protegida por la Directiva sobre Secretos Comerciales solo podrá ser divulgada bajo estrictas medidas de confidencialidad. En caso de controversias relacionadas con la compensación o las condiciones de acceso a datos, los Estados miembros podrán certificar organismos de resolución de disputas que ayudarán a las partes a alcanzar acuerdos justos y equilibrados.

Finalmente, la Ley de Datos aborda la equidad en los contratos de compartición de datos entre empresas, estableciendo un test de equidad contractual que protege a PYMEs y microempresas frente a términos contractuales abusivos. En caso de que una cláusula contractual no supere esta evaluación, no será vinculante para la parte más débil de la relación contractual. En su conjunto, este marco normativo representa un avance significativo en la gobernanza de datos dentro de la UE, al equilibrar el acceso y la protección de datos con el incentivo a la innovación y la competencia justa en la economía digital.

7.3.5.3. Espacios europeos de datos

Los Espacios Comunes Europeos de Datos buscan liberar el enorme potencial de la innovación basada en datos, permitiendo que los datos de toda la UE estén disponibles y se intercambien de manera segura y confiable. Empresas, administraciones públicas e individuos podrán controlar los datos que generan, beneficiándose al mismo tiempo de un marco seguro para compartirlos con fines de innovación. Estos espacios fomentarán el desarrollo de nuevos productos y servicios basados en datos, constituyendo la base de una economía digital interconectada y competitiva en Europa (43).

El desarrollo de estos espacios está impulsado por los actores de cada sector, quienes contribuyen a definir sus características y evolución. Sin embargo, todos los espacios de datos europeos comparten una infraestructura común y un marco de gobernanza que facilita la agrupación, el acceso y el intercambio de datos. Estos espacios se caracterizan por ser abiertos a la participación de cualquier organización o individuo, disponer de infraestructuras seguras y respetuosas con la privacidad para el acceso, procesamiento y uso de datos, contar con reglas de acceso justas, transparentes, proporcionales y no discriminatorias, respetar las normativas y valores de la UE en cuanto a protección de datos personales, derechos del consumidor y competencia, permitir que los titulares de datos concedan acceso o compartan determinados datos personales o no personales, y dar la posibilidad de que los datos se pongan a disposición para su reutilización, ya sea de forma gratuita o mediante compensación.

El concepto de espacio de datos aún es relativamente nuevo y carece de consenso total en cuanto a terminología y definiciones. Según la Comisión Europea, un espacio de datos es una infraestructura y marco de gobernanza que facilita la agrupación y el intercambio de datos (44). Otra definición del Centro de Soporte de Espacios de Datos (DSSC) lo describe como una plataforma que permite transacciones de datos entre diferentes actores de un ecosistema de datos en función de un marco de gobernanza específico (45). En esencia, los espacios de datos deben ser lo suficientemente flexibles para admitir múltiples casos de uso y facilitar la cooperación entre diferentes partes interesadas. En este contexto, un ecosistema de datos se entiende como un conjunto descentralizado de actores autónomos que comparten datos de manera colaborativa (46).

El término espacio de datos también se usa para referirse a la organización que administra el espacio y regula su gobernanza, denominada autoridad de gobernanza del espacio de datos. Por ejemplo, la Fundación Europeana gestiona el espacio de datos del patrimonio cultural de la UE (47). Esta autoridad de gobernanza puede cambiar con el tiempo, al igual que los servicios ofrecidos dentro del espacio de datos. El espacio en sí es la red de participantes y sus interacciones para compartir datos y servicios relacionados con los datos. Para diferenciar un espacio de datos plenamente operativo de una iniciativa en desarrollo, se emplea el término iniciativa de espacio de datos, que hace referencia a proyectos que están sentando las bases para la creación de futuros espacios de datos. Los espacios de datos financiados por la UE están diseñados para ser abiertos y accesibles para todos, sirviendo a sectores clave como la agricultura y el Pacto Verde Europeo.

El conjunto de los Espacios Comunes Europeos de Datos forma un único Espacio Común Europeo de Datos, similar al concepto de mercado único europeo. La idea es que los participantes puedan operar en todos los espacios bajo un marco de gobernanza común y con la menor fricción posible. Estos espacios están orientados a los servicios y centrados en el usuario, funcionando como mercados digitales donde los participantes pueden intercambiar datos y servicios relacionados. La gobernanza es llevada a cabo por una autoridad que establece y supervisa las normas, pero los servicios son proporcionados directamente por los participantes. Este modelo busca garantizar que los usuarios decidan el valor de su participación y que los espacios evolucionen conforme a sus necesidades.

Los espacios de datos también están diseñados para ser descentralizados, promoviendo una distribución del poder y la toma de decisiones entre múltiples participantes en lugar de una única autoridad central. La descentralización es uno de los cuatro principios fundamentales de los espacios de datos, junto con la soberanía de los datos, la igualdad de condiciones en el acceso a los datos y la gobernanza público-privada (46). No obstante, en la práctica, muchos espacios de datos aún operan bajo modelos centralizados, donde una única plataforma actúa como intermediaria de datos. Este enfoque, aunque ampliamente utilizado, conlleva el riesgo de generar nuevas formas de monopolio de datos.

Para mitigar estos riesgos, la Ley de Gobernanza de Datos establece regulaciones sobre intermediarios de datos, exigiendo la separación estructural entre los servicios de intermediación y otros servicios comerciales, prohibiendo la monetización directa de los datos y estableciendo normas estrictas para garantizar la neutralidad y evitar conflictos de interés. Estas medidas buscan prevenir la concentración excesiva de poder y fomentar un ecosistema de datos más abierto, equitativo y competitivo en la UE (48).

7.3.6. La Inteligencia Artificial

El AI Act, Reglamento (UE) 2024/1689 (49), es el primer marco jurídico integral a nivel mundial para la inteligencia artificial, cuyo propósito es mitigar los riesgos asociados a esta tecnología y consolidar el liderazgo de Europa en su regulación. Su enfoque se basa en una clasificación de riesgos y establece obligaciones específicas para desarrolladores y usuarios de IA, asegurando su uso confiable, seguro y centrado en el ser humano. Este marco legal forma parte de un conjunto de medidas más amplio, que incluye el Paquete de Innovación en IA, las Fábricas de IA y el Plan Coordinado en IA, con el objetivo de fortalecer la inversión, la innovación y la adopción de sistemas de IA dentro de la UE (50). Para facilitar la transición hacia este nuevo régimen normativo, la Comisión Europea ha lanzado el AI Pact (51), una iniciativa voluntaria que invita a desarrolladores y usuarios a cumplir anticipadamente con las principales disposiciones del AI Act.

El reglamento clasifica los sistemas de IA en cuatro niveles de riesgo:

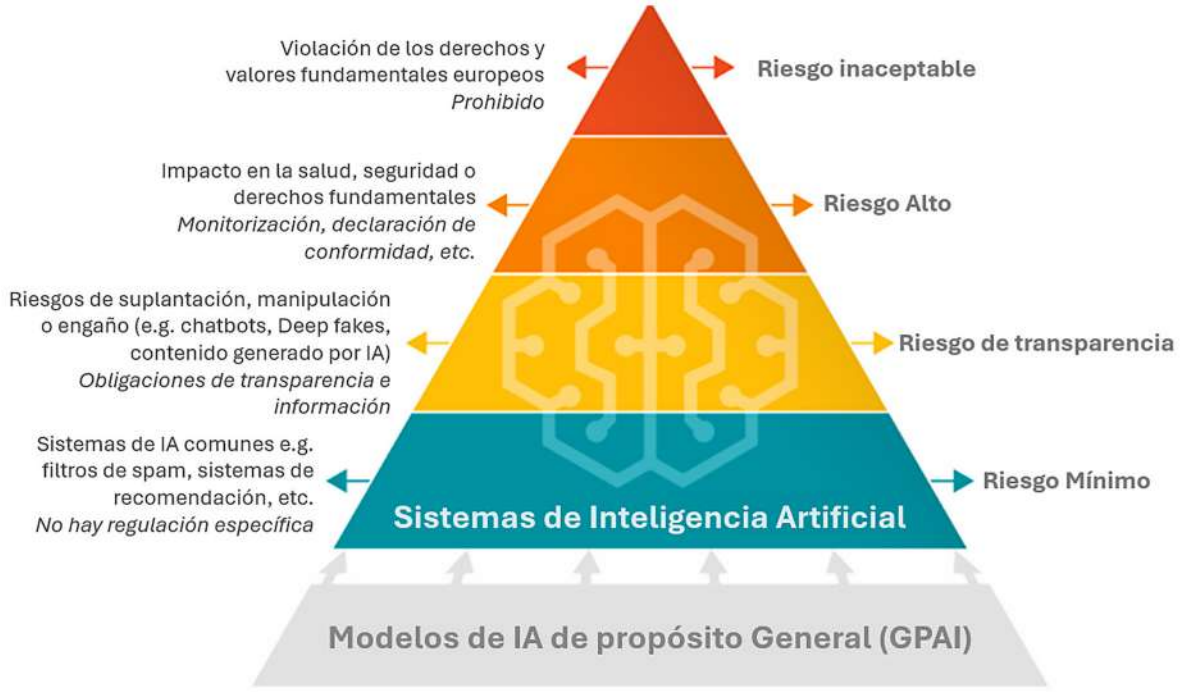


Figura 7.4.
Clasificación de los sistemas de IA de acuerdo con el riesgo.
Elaboración propia a partir de (52).

En el nivel de riesgo inaceptable, se prohíben aquellos sistemas que representen una amenaza evidente para la seguridad, los derechos fundamentales y la vida de las personas. Entre las prácticas prohibidas se incluyen la manipulación y el engaño mediante IA, la explotación de vulnerabilidades, la evaluación de riesgo delictivo individualizada, la creación de bases de datos de reconocimiento facial a partir de rastreo indiscriminado de datos en línea o CCTV, así como la identificación biométrica remota en tiempo real en espacios públicos con fines de aplicación de la ley. En el caso de los sistemas de alto riesgo, se consideran aquellas aplicaciones que pueden afectar la seguridad, la salud o los derechos fundamentales, tales como componentes de seguridad en infraestructuras críticas, evaluación de estudiantes en entornos educativos, IA en cirugía asistida por robots, herramientas de contratación y gestión laboral, evaluación de créditos y acceso a servicios esenciales, uso en la administración de justicia y procesos democráticos, así como aplicaciones en migración, asilo y control fronterizo. Para estos casos, se establecen requisitos estrictos antes de su comercialización, como evaluaciones de riesgo, transparencia en la documentación, supervisión humana, ciberseguridad y trazabilidad de resultados.

En cuanto a los sistemas de riesgo de transparencia, se imponen obligaciones de divulgación para garantizar la confianza del usuario. Se requiere, por ejemplo, que las personas sean informadas cuando interactúan con *chatbots* o sistemas generativos de IA, además de que el contenido generado por IA, como *deepfakes* o textos con fines informativos públicos, sea claramente identificable. Por otro lado, los sistemas de riesgo mínimo o inexistente, que incluyen aplicaciones como videojuegos basados en IA o filtros de *spam*, no están sujetos a restricciones específicas.

El AI Act entró en vigor el 1 de agosto de 2024 y será plenamente aplicable a partir del 2 de agosto de 2026, con excepciones para ciertas disposiciones que entrarán en vigor entre 2025 y 2027. Su ámbito de aplicación incluye tanto a actores públicos como privados, dentro y fuera de la UE, siempre que los sistemas de IA

sean comercializados o utilizados con impacto en ciudadanos europeos. Se establecen excepciones para actividades de investigación, desarrollo y prototipado, así como para sistemas diseñados exclusivamente para defensa y seguridad nacional. Las sanciones por incumplimiento pueden alcanzar hasta 35 millones de euros o el 7 % del volumen de negocios anual global, dependiendo de la gravedad de la infracción. Además, se prevé la imposición de multas a instituciones de la UE en caso de incumplimiento, bajo la supervisión del Supervisor Europeo de Protección de Datos.

El reglamento adopta un enfoque flexible y adaptable a los avances tecnológicos, permitiendo su modificación mediante actos delegados y la actualización de la lista de casos de alto riesgo. Se implementará un sistema de supervisión continua para evaluar la necesidad de ajustes normativos. Además, se fomenta la innovación mediante la creación de entornos de prueba regulados (*regulatory sandboxes*), donde las empresas pueden experimentar con nuevas tecnologías bajo condiciones controladas por un período de hasta 12 meses, sujeto a aprobación y supervisión de las autoridades competentes (52).

Por otra parte, se establecen obligaciones de transparencia para proveedores de modelos de IA de propósito general, exigiendo la divulgación de información clave para garantizar su seguridad y conformidad. Aquellos modelos con potencial riesgo sistémico deberán someterse a evaluaciones avanzadas y colaborar en la creación de un Código de Buenas Prácticas en conjunto con la Oficina de IA de la UE y otras partes interesadas (53).

7.4. UN NUEVO PLAN PARA LA PROSPERIDAD Y LA COMPETITIVIDAD SOSTENIBLES EN EUROPA

La Brújula de la Competitividad representa un esfuerzo integral de la Unión Europea para consolidar su liderazgo económico y tecnológico en un contexto global marcado por la aceleración de la digitalización, la transición ecológica y la creciente competencia internacional (54). En sintonía con otras iniciativas regulatorias y estratégicas, como el *AI Act*, la Ley de Datos y la Ley de Mercados Digitales, esta brújula busca garantizar que Europa no solo mantenga su posición en sectores clave, sino que también fortalezca su autonomía económica y reduzca vulnerabilidades frente a actores externos.

Una de sus prioridades es cerrar la brecha en innovación, fomentando un ecosistema que facilite la investigación y el desarrollo, permitiendo a las empresas europeas competir en igualdad de condiciones con otras potencias globales. Esto se traduce en un marco normativo más armonizado, con reglas claras que reduzcan la incertidumbre y favorezcan la inversión en sectores emergentes. La intersección con regulaciones como la Ley de Datos es evidente en la promoción de un entorno propicio para la economía digital, asegurando que las empresas cuenten con acceso a información de calidad para la innovación sin comprometer la privacidad y los derechos fundamentales de los ciudadanos.

La integración de políticas de descarbonización con estrategias económicas e industriales es otro de los pilares de la Brújula de la Competitividad, lo que refuerza la idea de un crecimiento sostenible. Esta alineación se refleja en el impulso a tecnologías limpias y en la promoción de la eficiencia energética dentro de las industrias clave, permitiendo a Europa liderar la transición hacia una economía neutra en carbono sin comprometer su competitividad. En este sentido, iniciativas como el Pacto Verde Europeo y la Ley de Industria Cero Neto establecen un marco de referencia para que las empresas adopten soluciones más sostenibles, complementando la regulación de la inteligencia artificial y otras tecnologías avanzadas.

Otro aspecto central es la reducción de dependencias estratégicas, con el objetivo

de reforzar la autonomía de la UE en sectores críticos como la energía, la digitalización y la fabricación avanzada. La capacidad de Europa para garantizar su seguridad económica está estrechamente vinculada con la regulación y supervisión de tecnologías clave, como la IA, los semiconductores y la biotecnología, evitando riesgos asociados a monopolios tecnológicos o vulnerabilidades en la cadena de suministro. En este contexto, la Ley de Chips desempeña un papel crucial al impulsar la producción europea de semiconductores, reduciendo la dependencia de mercados externos y garantizando la estabilidad en el desarrollo de infraestructura digital y sistemas inteligentes.

El impacto de esta iniciativa no se limita al ámbito empresarial, sino que también tiene implicaciones en el mercado laboral y en la estructura económica de la UE. Al fomentar la creación de empleos de alta calidad y reforzar la resiliencia económica, la Brújula de la Competitividad busca dotar a Europa de herramientas para afrontar desafíos globales sin comprometer su modelo social y económico. La combinación de incentivos para la innovación con una regulación equilibrada, como la propuesta en la Ley de Mercados Digitales, permite a las empresas aprovechar el potencial de nuevas tecnologías al tiempo que se minimizan los riesgos asociados a prácticas anticompetitivas en el sector digital.

7.5. CONCLUSIÓN

La evolución de la normativa digital en la Unión Europea refleja un esfuerzo continuo por consolidar un marco regulador que garantice la protección de los derechos fundamentales de los ciudadanos en el entorno digital, al tiempo que fomenta la innovación y la competitividad. Desde la adopción del RGPD y la Directiva de Comercio Electrónico hasta las recientes normativas de la Década Digital, la UE ha desarrollado un enfoque basado en la transparencia, la seguridad jurídica y la responsabilidad de los actores digitales.

La estrategia de la UE en materia digital ha demostrado que es posible establecer un marco regulador sólido sin frenar el desarrollo tecnológico. Sin embargo, el reto radica en encontrar un equilibrio que permita incentivar la inversión y el crecimiento de empresas europeas en un entorno global altamente competitivo. La regulación debe seguir evolucionando para adaptarse a nuevas realidades tecnológicas sin imponer barreras excesivas que puedan ralentizar la innovación y la competitividad de la industria digital europea.

7.6. REFERENCIAS BIBLIOGRÁFICAS

1. Reglamento (UE) 2016/679 general de protección de datos [Internet]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679
2. Wolford B. What is GDPR, the EU's new data protection law? [Internet]. GDPR.EU; 2025 [citado 30 de marzo de 2025]. Disponible en: https://gdpr.eu/what-is-gdpr/
3. Consejo Europeo. Reglamento General de Protección de Datos [Internet]. 2024 jun 13 [citado 30 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/es/policies/data-protection-regulation/
4. Comisión Europea. Legal framework of EU data protection [Internet]. 2025 [citado 30 de marzo de 2025]. Disponible en: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en?lang=en&prefLang=es

5. European Data Protection Board. The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC [Internet]. 2019 ene 21 [citado 30 de marzo de 2025]. Disponible en: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

6. European Data Protection Board. 1.2 billion euro fine for Facebook as a result of EDPB binding decision [Internet]. 2023 may 22 [citado 30 de marzo de 2025]. Disponible en: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

7. Directive 2000/31/EC on electronic commerce [Internet]. Disponible en: https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

8. Comisión Europea. Directiva sobre el comercio electrónico [Internet]. 2025 ene 22 [citado 30 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/e-commerce-directive

9. de Streel A, Husovec, M. The e-commerce Directive as the cornerstone of the Internal Market [Internet]. D.-G. f. Policies Ed.; 2020 may [citado 30 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU%282020%29648797_EN.pdf

10. von der Leyen, U. A Union that strives for more. My agenda for Europe [Internet]. European Commission; 2019 jul 16. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_en

11. Comisión Europea. Reglamento de servicios digitales [Internet]. 2022 oct 19 [citado 03 de marzo de 2025]. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_es

12. Consejo Europeo. Reglamento de Servicios Digitales [Internet]. 2025 feb 04 [citado 03 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/es/policies/digital-services-act/

13. Parlamento Europeo. Dos leyes históricas para unos servicios digitales más seguros y abiertos [Internet]. 2022 jul 05 [citado 03 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/news/es/press-room/20220701IPR34364/dos-leyes-historicas-para-unos-servicios-digitales-mas-seguros-y-abiertos

14. Comisión Europea. Una Europa Adaptada a la Era Digital: nuevas normas para las plataformas en línea. 2022 oct 19 [citado 03 de marzo de 2025]. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act/europe-fit-digital-age-new-online-rules-platforms_es

15. Unión Europea. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) [Internet]. 2022 oct 19 [citado 03 de marzo de 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R2065

16. Parlamento Europeo. Digital Markets Act [Internet]. 2022 nov [citado 21 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf

17. Comisión Europea. Acerca de la Ley de Mercados Digitales [Internet]. 2025 [citado 21 de marzo de 2025] Disponible en: https://digital-markets-act.ec.europa.eu/about-dma_en?prefLang=es&etrans=es

18. Unión Europea. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [Internet]. 2022 sep 14 [citado 21 de marzo de 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925

19. Comisión Europea. Ley de Mercados Digitales [Internet]. 2025 [citado 21 de marzo de 2025]. Disponible en: https://digital-markets-act.ec.europa.eu/index_en?prefLang=es&etrans=es

20. Comisión Europea. Gatekeepers [Internet]. 2024 may 13 [citado 27 de marzo de 2025]. Disponible en: https://digital-markets-act.ec.europa.eu/gatekeepers_en

21. Unión Europea. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Internet]. 2014 jul 23 [citado 21 de marzo de 2025]. Disponible en: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

22. Parlamento Europeo. Revision of the eIDAS Regulation. Findings on its implementation and application. 2022 mar [citado 21 de marzo de 2025] Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf

23. State of the Union Address by President Ursula von der Leyen [Internet]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

24. COM(2021) 118 [Internet]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52021DC0118

25. Jerković R. Revision of the eIDAS Regulation – European Digital Identity (EUid) [Internet]. Parlamento Europeo; 2025 feb 20 [citado 21 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid?sid=8901

26. Comisión Europea. Ley Europea de Chips [Internet]. 2023 sep [citado 27 de marzo de 2025]. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_es

27. Ragonnaud G. The EU chips act. Securing Europe's supply of semiconductors [Internet]. 2023 jun [citado 27 de marzo de 2025] Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733596/EPRS_BRI(2022)733596_EN.pdf

28. Consejo Europeo. The EU chips industry [Internet]. 2025 mar 14 [citado 27 de marzo de 2025]. Disponible en: https://www.consilium.europa.eu/en/policies/eu-chips-industry/#act

29. Comisión Europea. Discurso sobre el estado de la Unión pronunciado por la presidenta Ursula von der Leyen [Internet]. 2021 sep 15. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/speech_21_4701

30. Comisión Europea. Discurso sobre el estado de la Unión de la presidenta Ursula von der Leyen [Internet]. 2022 sep 13. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/SPEECH_22_5493

31. EUR-Lex. COM/2013/0298 final [Internet]. 2013. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013DC0298

32. SWD(2022) 147 final. Commission Staff Working Document - A Chips Act for Europe [Internet]. 2022 may 11 [citado 27 de marzo de 2025]. Disponible en: https://ec.europa.eu/newsroom/dae/redirection/document/86690

33. Comisión Europea. International trade and production of high-tech products - Statistics Explained [Internet]. 2024. Disponible en: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_and_production_of_high-tech_products

34. COM(2020) 66 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos [Internet]. 2020 feb [citado 27 de marzo de 2025]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066

35. COM(2019) 640 final [Internet]. 2019. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0640

36. Data.europa.eu Academy. Navigating the European data strategy: the progress towards the single market of data [Internet]. 2025 ene. Disponible en: https://data.europa.eu/sites/default/files/course/Webinar%20data%20policies%20-%20slidedeck%20%281%29.pdf

37. Regulation (EU) 2022/868 [Internet]. 2022. Disponible en: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

38. Martínez R. La Guía de la Unión Europea para el despliegue de la Data Governance Act: servicios de intermediación del sector público [Internet]. datos.gob.es; 2025 ene 29 [citado 27 de marzo de 2025]. Disponible en: https://datos.gob.es/es/blog/la-guia-de-la-union-europea-para-el-despliegue-de-la-data-governance-act-servicios-de

39. Comisión Europea. Explicación de la Ley de Gobernanza de Datos [Internet]. 2024 oct 11 [citado 27 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/data-governance-act-explained

40. Regulation (EU) 2023/2854 Data Act [Internet]. Disponible en: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

41. Comisión Europea. Ley de Datos [Internet]. 2024 oct 10 [citado 28 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/data-act

42. Madiega T. The data act [Internet]. 2023 may [citado 28 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI(2022)733681_EN.pdf

43. Comisión Europea. Common European Data Spaces [Internet]. 2025 mar 27 [citado 29 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/data-spaces

44. SWD(2022) 45 final Commission Staff Working Document on Common European Data Spaces [Internet]. Disponible en: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

45. DSSC Glossary Version 1.0 | March 2023 [Internet]. Disponible en: https://dataspacessupportcentre.refined.site/space/Glossary/55443460/DSSC+Glossary+%7C+Version+1.0+%7C+March+2023?attachment=/rest/api/content/55443460/child/attachment/att110362680/download&type=application/pdf&filename=DSSC-Data-Spaces-Glossary-v1.0.pdf

46. Page M, Cecconi G. European data spaces and the role of data.europa.eu [Internet]. Luxemburgo: Publications Office of the European Union; 2023. DOI:10.2830/1603

47. Europeana. Discover Europe's digital cultural heritage [Internet]. Disponible en: https://www.europeana.eu/en

48. Farrell E, Minghini M, Kotsev A, Soler-Garrido J, Tapsall B, Micheli M, Bernal J, et al. European Data Spaces: Scientific insights into data sharing and utilisation at scale [Internet]. Luxemburgo: Publications Office of the European Union; 2023. DOI:10.2760/400188

49. Unión Europea. Regulation (EU) 2024/1689 AI Act [Internet]. Disponible en: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

50. Comisión Europea. AI Act [Internet]. 2025 feb 18 [citado 29 de marzo de 2025]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

51. AI Act | Shaping Europe's digital future [Internet]. Disponible en: https://digital-strategy.ec.europa.eu/en

52. Madiega T. Artificial intelligence act [Internet]. 2024 sep [citado 29 de marzo de 2025]. Disponible en: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

53. Código de buenas prácticas de la IA de finalidad general [Internet]. Configurar el futuro digital de Europa. 2025. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/ai-code-practice

54. COM(2025) 30 final. A Competitiveness Compass for the EU [Internet]. Disponible en: https://commission.europa.eu/document/download/10017eb1-4722-4333-add2-e0ed18105a34_en

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico

Cofinanciado por la Unión Europea

8

Prospectiva sobre el impacto de la inteligencia artificial en los derechos de los ciudadanos

Moisés Barrio Andrés

8.1. INTRODUCCIÓN

Las nuevas fronteras del Derecho y de los derechos hoy en día están representadas por el potencial de la Inteligencia Artificial (IA), es decir, la enorme capacidad de recopilar, sistematizar y procesar datos para producir algoritmos capaces de encontrar soluciones "inteligentes" para resolver problemas, o para tomar decisiones de forma autónoma e imparcial. Datos relativos a las personas, pero también a bienes, servicios, mercancías o capacidades de producción, que pueden intercambiarse creando así un verdadero mercado de datos. Y, sobre todo, se pueden procesar de forma autónoma sin intervención humana. De esta manera, terminan produciendo cambios en la realidad, aprendiendo elementos cognitivos y resolviendo soluciones a problemas de una manera muy rápida, que las capacidades intelectuales humanas no serían capaces de hacer ni tan bien ni tan rápido.

La IA produce un formidable impacto en todas las ciencias del conocimiento humano, perfilándolas artificialmente. También en el Derecho, que tendrá que remodelar cada vez más sus paradigmas, teniendo en cuenta el uso de sistemas de IA para ayudar a mejorar las sentencias judiciales o para desarrollar actos administrativos objetivos, por citar solo algunos ejemplos. Por supuesto, el Derecho hace tiempo que entró en la sociedad tecnológica, es decir, el inicial Ciberderecho (1) y ahora Derecho digital. Por lo tanto, el antiguo brocardo probablemente de origen medieval podría reformularse como *ubi societas technologica, ibi ius*. De hecho, los nuevos espacios de relación y conflicto en el ámbito de la IA nos llevaron a algunos autores primero, y después a los Estados más avanzados por medio de múltiples iniciativas jurídicas a establecer unos postulados regulatorios que pueden sintetizarse, en último término, en un principio de precaución (2), inspirado en el Derecho del medio ambiente y esbozado de la siguiente manera: la condición de incertidumbre sobre los posibles efectos negativos del uso de la IA no puede ser desechada como una razón legítima para no regular y encauzar dicha supertecnología, en el marco de los principios del Estado Constitucional de Derecho.

Por lo tanto, la protección de los bienes constitucionales debe anticiparse con respecto a la producción real de daños causados por la tecnología. El parámetro para juzgar el fenómeno de la IA es la Constitución y, más en general, el constitucionalismo, especialmente en la parte en que establece y protege la suprema dignidad de la persona humana (art. 10 de la Constitución Española de 1978, art. 1 de la Carta de Derechos Fundamentales de la Unión Europea).

Así lo ha entendido, como veremos a renglón seguido, el legislador europeo con el Reglamento de Inteligencia Artificial, y lo establece explícitamente en su considerando 8:

"En consecuencia, se necesita un marco jurídico de la Unión que establezca unas normas armonizadas en materia de IA para impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado, la puesta en servicio y la utilización de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de libre circulación de mercancías y servicios. Esas normas deben ser claras y firmes por lo que respecta a proteger los derechos fundamentales, apoyar nuevas soluciones innovadoras, posibilitar un ecosistema europeo de agentes públicos y privados que creen sistemas de IA en consonancia con los valores de la Unión y liberar el potencial de la transformación digital en todas las regiones de la Unión [...]".

Y es que la última década nos ha traído unos avances revolucionarios en la disciplina de la

inteligencia artificial (3), que han impulsado la aprobación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial (4) (5), el RIA en lo sucesivo).

Estos avances pueden condensarse en tres hitos. El primero se produjo con la evolución de los modelos tradicionales de aprendizaje automático (el tradicional *machine learning*) a comienzos de este siglo. Estos modelos a menudo se entrenan utilizando un conjunto de datos etiquetados (o clasificados) de características significativas para aprender relaciones desconocidas entre variables de entrada y de salida. El proceso de entrenamiento determina los valores (o pesos) óptimos de los parámetros relacionados del modelo y, a su vez, permite realizar tareas de tipo predictivo (por ejemplo, clasificación de nuevos datos no analizados con anterioridad o previsión de valores desconocidos). Esta categoría de sistemas de IA se conoce como modelos orientados a tareas —u orientados a características—, que a menudo logran un rendimiento razonable en términos de precisión de la predicción cuando se utiliza un conjunto de datos de calidad óptima y una complejidad sustancial del modelo. Su limitación técnica, sin embargo, es que se requiere un nuevo conjunto de datos etiquetados y un nuevo modelo para cada tarea única, lo que da lugar a procesos computacionales de entrenamiento intensivos y lentos. Y es que la dependencia del modelo con respecto a la singularidad de la tarea para la que se entrena es a menudo tan significativa que, por ejemplo, un modelo de alto rendimiento que detecta tumores cerebrales en un TAC no puede aplicarse a la detección del fraude fiscal.

El segundo hito comenzó con la introducción del aprendizaje profundo (o *deep learning*) a principios de la década de 2010, combinado con la técnica del aprendizaje por transferencia. En el aprendizaje por transferencia, a diferencia de los modelos de aprendizaje automático tradicionales, los modelos de aprendizaje profundo se entrenan con grandes conjuntos de datos para realizar una determinada tarea, pero luego se adaptan para realizar nuevas tareas mediante el ajuste preciso necesario de los parámetros del modelo (el *fine tuning*), en lugar de tener que entrenar un modelo completamente nuevo desde cero. Aquí surgen las redes neuronales convolucionales, que buscan imitar el funcionamiento y la estructura de las redes neuronales cerebrales del ser humano. Están formadas por nodos interconectados que reciben información, la procesan y la pasan a través de otra neurona artificial. Estos nodos también se conocen como neuronas artificiales, que se pueden programar para optimizar la salida y, por tanto, se adaptan a los diferentes tipos de entradas. Estas redes inicialmente estaban enfocadas en la identificación de objetos en imágenes. Posteriormente, este enfoque se generalizó a otros tipos de datos referidos a texto, voz, etc. Además de adaptarse a otras aplicaciones, una característica destacada de los modelos de *deep learning* en comparación con los modelos de *machine learning* es su mejor rendimiento atribuido a la mayor escala de los datos utilizados para el entrenamiento y a una arquitectura más profunda de los modelos que abarca millones de parámetros. Ahora bien, todavía estos sistemas de IA siguen estando centrados en el modelo.

El tercer hito surge especialmente en la década de 2020, cuando se hace viable un enfoque de sistemas de IA centrados en los datos que utiliza modelos de base o fundacionales (los *foundation models*). Esta categoría de sistemas de IA aún está en desarrollo. En lugar de modelos más profundos con arquitecturas más potentes, los modelos fundacionales hacen uso de los métodos de *machine learning* existentes, como el aprendizaje supervisado, no supervisado y transferido, para analizar una cantidad de datos sin precedentes a través de la computación a gran escala (así, los contenidos publicados en abierto en Internet que figuran en repositorios como Common Crawl). En sus propias palabras, los defensores (6) del paradigma de los modelos fundacionales proclaman que "el aprendizaje de transferencia es lo que hace posibles los

modelos fundacionales, pero la escala es lo que los hace potentes". Técnicamente, se caracterizan por dos atributos clave: la autonomía y la homogeneización. La **autonomía** se refiere al proceso de lograr un determinado comportamiento del modelo a través de la inducción de información dentro del modelo, en lugar de construirlo explícitamente a través de, por ejemplo, la arquitectura o el diseño del modelo. Esto significa que el modelo produce sus resultados a medida que emergen a través del descubrimiento de conocimientos dentro de los datos de entrenamiento, lo que posteriormente desplaza el foco de atención del diseño del modelo a los datos de entrenamiento (por lo tanto, es un sistema centrado en los datos). La **homogeneización** alude a la idea de que un modelo genérico fundacional puede aplicarse a una amplia gama de aplicaciones, en lugar de desarrollar múltiples modelos para tareas específicas. La consecuencia de la homogeneización es la ausencia de dependencia del modelo con respecto a la tarea, como ocurría con los sistemas tradicionales de IA. El resultado es una mejora significativa de la generalizabilidad gracias a la necesaria adaptación a aplicaciones más amplias. Probablemente, la aplicación más notable de este tipo de sistemas son los grandes modelos lingüísticos (LLM, por sus siglas inglesas de *Large Language Models*), base de aplicaciones como ChatGPT de OpenAI, que toman las preguntas de los usuarios como un estímulo de entrada y aprovechan sus capacidades de autonomía para responder a una amplia variedad de preguntas en una narrativa similar a la humana (7).

Aunque el poderoso potencial de la IA de nueva generación se ha introducido con éxito a partir del 30 de noviembre de 2022 con el lanzamiento de ChatGPT, siguen abiertas las preocupaciones en torno a la transparencia, la seguridad, la confianza, los derechos fundamentales (por ejemplo, la discriminación y la protección de datos), así como la sostenibilidad y el uso de la energía. A nivel de la Unión Europea (UE), estos desafíos aspiran a ser resueltos por medio del señalado RIA. Con carácter general, el Reglamento será aplicable a partir del 2 de agosto de 2026, con las excepciones previstas en su artículo 113. Y establece además unos plazos aplicativos progresivos de seis meses para los usos prohibidos y disposiciones generales de la norma (2 de febrero de 2025), de un año (2 de agosto de 2025) para autoridades notificantes y organismos notificados, modelos de uso general, gobernanza y régimen sancionador; y, por último, tres años (2 de agosto de 2027) para el cumplimiento derivado de las obligaciones de los sistemas de alto riesgo.

También existe una regulación jurídica menos ambiciosa en países como Estados Unidos, la República Popular China o Brasil. Organizaciones intergubernamentales como la Organización de Cooperación y Desarrollo Económicos (OCDE) o los países del G7 han emitido determinadas recomendaciones no vinculantes. Del mismo modo, el Consejo de Europa, con el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, adoptado el 17 de mayo de 2024 y firmado por la Unión Europea, Estados Unidos y el Reino Unido, entre otros, ha propuesto el primer tratado internacional en la materia, que establece un marco jurídico que abarca todo el ciclo de vida de los sistemas de IA y que se ocupa de los riesgos que estos pueden plantear, a la vez que promueve la innovación responsable. El convenio adopta un enfoque basado en el riesgo para diseñar, desarrollar, usar y decomisar sistemas de IA, que exige considerar cuidadosamente cualquier posible consecuencia negativa del uso de sistemas de IA.

Por eso, el RIA con su enfoque amplio horizontal, sus disposiciones más detalladas y su carácter jurídicamente vinculante, ocupa la posición más destacada a nivel de Derecho comparado. El RIA está destinado a convertirse en una referencia mundial para la regulación de la IA, una nueva manifestación del llamado "efecto Bruselas", convirtiendo al Reglamento en la referencia normativa en este ámbito regulador de importancia estratégica, como ocurrió en el pasado con la protección de datos. Ahora bien, su elaboración ha sido resultado de un complejo camino iniciado en 2017.

8.2. EL CAMINO HACIA EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

En los últimos años, garantizar la seguridad de la IA se ha consolidado como una preocupación de estudio interdisciplinar que va más allá de las consideraciones éticas. Se han llevado a cabo así múltiples estudios sobre la transparencia y la explicabilidad de las decisiones tomadas por los sistemas de IA, el potencial de discriminación o injusticia en el uso de estos sistemas, y los retos para controlar y alinear los sistemas de IA con los derechos fundamentales. Existe una necesidad acuciante de garantizar la solidez y la calidad técnica de la IA. Las prácticas extractivas tanto de datos (algunos de ellos protegidos por derechos de propiedad intelectual) como de minerales y el consumo energético de la IA también son motivo de preocupación.

Por eso, juristas y políticos han empezado a plantearse leyes para hacer frente a los múltiples retos de la IA. Las cuestiones que se suscitan son diversas y tienen una repercusión sustancial en los derechos fundamentales (libertad, trabajo y empleo, intimidad, igualdad y no discriminación, participación democrática, tutela judicial efectiva, libertad de expresión e información, organización administrativa, protección del medio ambiente), pero también en la responsabilidad civil y penal, la protección de los datos personales, la intimidad y los derechos de la personalidad, la propiedad intelectual, el Derecho de la competencia, el Derecho del medio ambiente, el Derecho penal, el Derecho tributario y el Derecho público en general.

Aunque se están llevando a cabo iniciativas reguladoras en todo el mundo, la Unión Europea ha tomado la delantera. Ya el 16 de febrero de 2017, el Parlamento Europeo adoptó una resolución con recomendaciones a la Comisión Europea sobre normas de Derecho civil en materia de robótica (8). Esta resolución reconoce los peligros y oportunidades de la robótica y la inteligencia artificial y formula varias propuestas para su regulación, instando a la Comisión Europea a presentar una propuesta legislativa sobre las cuestiones jurídicas relacionadas con el desarrollo y uso de las mismas (9). A este documento se anexaron recomendaciones sobre el contenido de dicha propuesta —incluida la definición de robot, la creación de un sistema de registro gestionado por una agencia europea, normas sobre responsabilidad civil, seguros y fondos de garantía y el establecimiento de normas de interoperabilidad— y una "Carta sobre robótica", es decir, un código de conducta voluntario dirigido a investigadores y diseñadores de robots. Esta resolución de 2017 aceleró el debate sobre las cuestiones jurídicas relacionadas con la inteligencia artificial y la robótica.

Al año siguiente, la Comisión Europea presentó dos comunicaciones: "Inteligencia Artificial para Europa", del 25 de abril de 2018 (10), y el "Plan Coordinado sobre la inteligencia artificial", de 7 de diciembre de 2018 (11). Siguieron otras resoluciones, estudios e informes, y el "Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza", presentado por la Comisión con fecha 19 de febrero de 2020 (12), fijó el enfoque de las ulteriores propuestas normativas.

El 20 de octubre de 2020, el Parlamento Europeo adoptó una resolución con recomendaciones a la Comisión sobre el régimen de responsabilidad civil aplicable a la inteligencia artificial (13). Este documento contenía el texto de un proyecto de reglamento sobre la responsabilidad por el funcionamiento de los sistemas de IA (14). El 28 de septiembre de 2022, la Comisión Europea presentó dos propuestas normativas: una revisión de la Directiva sobre responsabilidad por productos defectuosos, que pretende sustituir a la hasta ahora vigente Directiva 85/374/CE (15), y una nueva Directiva sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (16). La primera de ellas ha sido ya aprobada como Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo.

Sin embargo, el principal instrumento normativo regulador de esta tecnología es el Reglamento (UE) de Inteligencia Artificial, el indicado RIA. Este Reglamento se deriva de una propuesta presentada por la Comisión Europea el 21 de abril de 2021 (17). La propuesta fue objeto de intensas negociaciones (incluida una maratón de 36 horas entre representantes de la Comisión Europea, el Parlamento Europeo y el Consejo), enmiendas de gran alcance y una corrección de errores (19 de abril de 2024), se aprobó el 13 de junio de 2024 y se publicó el 12 de julio de 2024 en el DOUE con el número de Reglamento (UE) 2024/1689.

8.3. EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL Y SU OBJETO

El propósito del Reglamento es proporcionar seguridad jurídica mediante un marco unificado previo o *ex ante* aplicable a todos los sistemas de IA puestos en el mercado de la Unión, y lo hace con distintos niveles de obligaciones en atención al grado de riesgo que presenta cada sistema para la salud, la seguridad y los derechos fundamentales de los ciudadanos. Para la norma, el riesgo es "la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio" (art. 3.2 RIA). Este enfoque basado en el riesgo lleva al RIA a prohibir determinados usos considerados de riesgo inaceptable en la UE, imponer obligaciones estrictas para usos de riesgo alto, establecer obligaciones de transparencia para ciertos sistemas de riesgo limitado, y dejar sin regulación imperativa al resto de sistemas de riesgo mínimo.

Contrariamente a los enfoques regulatorios sectoriales o verticales, como ocurre en el Derecho norteamericano en esta materia con la Orden ejecutiva del presidente Biden sobre el desarrollo y la utilización seguros y fiables de la inteligencia artificial, de 30 de octubre de 2023, el RIA establece normas claras para todos los sistemas y ámbitos de aplicación de la IA. Por eso, el RIA tiene un carácter horizontal —es decir, no limitado a sectores concretos—, y pretende dar una respuesta proporcional al riesgo generado por los sistemas de IA. Y lo hace en forma de reglamento europeo, que es directamente aplicable en todos los Estados miembros (art. 288 TFUE), sin necesidad de normas nacionales de transposición como sucede con las directivas.

Además, el RIA también condiciona la identificación de siete principios como directrices genéricas a tener en cuenta en el diseño de una IA coherente, fiable y centrada en el ser humano, respetuosa con los derechos fundamentales y con los valores de la UE: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental, y rendición de cuentas (cdo. 27 RIA).

Ahora bien, el RIA no agota la regulación de la IA. El mismo debe aplicarse de forma conjunta con el Derecho digital europeo general (18) (RGPD (19), DSA (20), DMA (21), NIS2 (22)…), así como con las normas sectoriales que resulten de aplicación (por ejemplo, sector financiero, drones o dispositivos médicos). Ese criterio sobre la interacción entre el RIA y otros instrumentos del Derecho de la Unión y de los ordenamientos jurídicos de los Estados miembros tiene reflejo en su artículo 2. Se destaca expresamente que el Reglamento no afecta al RGPD ni a la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, que resultan plenamente aplicables (art. 2.7 RIA).

Asimismo, y en cuanto a los eventuales daños que puedan surgir *ex post*, ya sabemos que con fecha 28 de septiembre de 2022 la Comisión Europea publicó dos Propuestas de Directiva que completarán el régimen europeo en la materia:

a) La primera propuesta, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), pretende facilitar

la prueba de la culpa y de la relación de causalidad en el caso de daños causados por sistemas de inteligencia artificial que deban resolverse de acuerdo con las respectivas legislaciones nacionales de responsabilidad por culpa. A fecha de escribir estas líneas no ha sido aprobada.

b) La segunda propuesta, que ya es norma jurídica en virtud de la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. Tiene por objeto sustituir la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, que ha estado vigente hasta 2024, por una nueva regulación adaptada a las nuevas necesidades de la IA y, de paso, de la economía circular.

Una limitación significativa con respecto al alcance práctico del RIA es que no se aplica a las personas físicas que utilizan sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional (arts. 2.10 y 3.4 RIA), en la línea de lo previsto con respecto al ámbito de aplicación material en otros instrumentos como el RGPD, cuyo artículo 2.2.c precisa que no se aplica al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Además, para contribuir a fomentar la innovación, el RIA tampoco se aplica a los sistemas o modelos de IA desarrollados y puestos en servicio "específicamente con la investigación y el desarrollo científicos como única finalidad" (art. 2.6 RIA), ni a las actividades de investigación, prueba o desarrollo relativas a sistemas modelos de IA antes de su introducción en el mercado o puesta en servicio (art. 2.8 RIA).

Otras exclusiones relevantes del ámbito de aplicación material del RIA en su artículo 2 van referidas a que esta norma no es aplicable a los sistemas de IA en la medida en que se introduzcan en el mercado, se pongan en servicio o se utilicen exclusivamente con fines militares, de defensa o de seguridad nacional. Además, tampoco afecta a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias.

El RIA se articula fundamentalmente sobre la base jurídica del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que faculta a la Unión para la adopción de medidas para garantizar el establecimiento y funcionamiento del mercado interior, conforme a los principios de subsidiariedad y proporcionalidad. A esta base se añadió luego el artículo 16 del TFUE (protección de datos personales). Precisamente, evitar esa fragmentación justifica la adopción de un marco armonizado que asegure a nivel de la Unión la libre circulación de mercancías y servicios basados en la IA.

Así, la propuesta original del Reglamento se refería principalmente a la armonización del marco jurídico para la adopción y el uso de los sistemas de IA en el mercado único de la UE (la base jurídica principal del RIA era —y sigue siendo— el artículo 114 del TFUE relativo a la armonización del mercado, junto con el artículo 16 del TFUE relativo a la protección de datos). Esto también significa que el RIA se centra en "la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión" (art. 1.2.a RIA), lo que tiene como consecuencia que los sistemas de IA destinados exclusivamente a la búsqueda y el desarrollo científicos quedan fuera de su ámbito de aplicación (véase también el cdo. 25).

No obstante, este enfoque de la seguridad de los productos suscitó críticas de la sociedad civil y de algunos académicos que exigimos más atención a los aspectos de los derechos fundamentales, en concreto a los posibles daños individuales o colectivos derivados del despliegue de la IA. El Parlamento Europeo inició un intento de replantear los objetivos del RIA en esta dirección a lo largo de 2023 en sus enmiendas. En última instancia, el texto final del RIA puede considerarse un reglamento híbrido,

en el que la mayoría de sus disposiciones siguen centrándose en la seguridad de los productos, la normalización y la protección de los consumidores. Sin embargo, otras disposiciones, como las relativas a los riesgos inaceptables (las "prácticas de IA prohibidas") del artículo 5 del RIA, se adentran en los ámbitos de la no discriminación, la protección de datos e incluso el derecho procesal penal, cuando se trata de salvaguardias contra el uso indebido de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de garantía del cumplimiento del Derecho.

El RIA tiene, según su artículo 1.1, el siguiente objeto: "mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, "sistemas de IA") en la Unión así como prestar apoyo a la innovación".

Es decir, la norma pretende promover la adopción de la inteligencia artificial centrada en el ser humano y fiable, garantizando al mismo tiempo un alto nivel de protección de la salud, la seguridad, los derechos fundamentales y la protección del medio ambiente contra los efectos nocivos de los sistemas de inteligencia artificial en la Unión, y apoyando también la innovación. El objetivo es regular todo el ciclo de vida de los sistemas de IA, desde la recogida de datos de entrada hasta su uso final.

Para ello, el Reglamento establece (art. 1.2 RIA):

a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión;

b) prohibiciones de determinadas prácticas de IA;

c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas;

d) normas armonizadas de transparencia aplicables a determinados sistemas de IA;

e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general;

f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento; y

g) medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes (las *startups*).

Por tanto, y como característica distintiva del RIA, se positiviza a escala de toda la Unión Europea una regulación por capas o niveles de riesgo, donde no se regula la tecnología en sí sino los ámbitos de uso concretos, con el objetivo de abordar los riesgos a la salud, seguridad y derechos fundamentales asociados a su finalidad prevista del concreto sistema de IA. Por eso, la intensidad regulatoria que incorpora la norma está adaptada al nivel de riesgo del concreto sistema de inteligencia artificial sobre la salud, la seguridad y los derechos fundamentales del usuario. Es muy diferente la regulación que tiene un coche autónomo (sistema de alto riesgo) o el corrector ortográfico de Microsoft Word (sistema de riesgo mínimo sin regulación imperativa), por ejemplo. Y el RIA centra su densidad regulatoria en aquellos supuestos en los que estas nuevas herramientas de IA suscitan riesgos no resueltos de manera adecuada por el ordenamiento jurídico existente.

La aplicación de esta norma será responsabilidad de una serie de entidades públicas nacionales y de la Unión Europea.

Los Estados miembros deberán crear o designar, al menos, una autoridad de vigilancia del mercado y una autoridad de notificación para garantizar la aplicación y ejecución del RIA. España se ha adelantado a su entrada en vigor de forma pionera en la UE con la creación de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) (19). La AESIA fue creada en virtud de la disposición adicional séptima de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes. Y su Estatuto ha sido aprobado por Real Decreto 729/2023, de 22 de agosto.

En la Unión Europea, por su parte, la aplicación del RIA contará con el apoyo de una serie de organismos, como la Comisión Europea, el Consejo Europeo de Inteligencia Artificial, la Oficina Europea de IA, los organismos de normalización de la UE (CEN, Comité Europeo de Normalización; CENELEC, Comité Europeo de Normalización Electrotécnica y ETSI, Instituto Europeo de Normas de Telecomunicaciones que corresponde a sus siglas en inglés), un foro consultivo y un grupo de expertos científicos independientes. La Oficina de la IA de la UE ha sido concebida, entre otros fines, para asesorar sobre la aplicación de este nuevo grupo normativo regulador de la IA, en particular por lo que respecta a los modelos de IA de uso general, y para elaborar códigos de buenas prácticas que respalden la correcta aplicación del Reglamento.

8.4. EL MODELO REGULATORIO DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

El RIA, como sabemos, sigue un enfoque basado en el riesgo que clasifica en cuatro categorías diferentes los riesgos de la IA.

Esta clasificación jurídica cuatripartita de los riesgos comprende, en primer lugar, los sistemas "prohibidos" (art. 5 RIA). Son aquellos que infringen o no garantizan la observancia de los derechos fundamentales de las personas (así, porque manipulan subliminalmente el comportamiento humano causando daños, o se aprovechan de la vulnerabilidad por razones de edad, discapacidad o de una situación social o económica específica de una persona o de un grupo, por ejemplo).

En segundo lugar, figuran los sistemas de "alto riesgo" (art. 6 RIA). Se trata de los sistemas que pueden tener efectos perjudiciales para la salud, la seguridad o los derechos fundamentales de las personas (ya sean componentes de seguridad de productos cubiertos por la legislación armonizada europea de seguridad de productos —máquinas, juguetes, ascensores, productos sanitarios…—, o bien estén clasificados *ex lege* por el Reglamento en su anexo III —sistemas de identificación biométrica remota, sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras críticas, sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes…—). Dichos sistemas están autorizados, pero sujetos a una serie de requisitos y obligaciones imperativos para acceder al mercado de la UE y que conforman el grueso de la norma.

A renglón seguido figuran los sistemas de "riesgo limitado" (art. 50 RIA). Se trata de aquellos sistemas que presentan riesgos limitados por su falta de transparencia (así, *chatbots* o robots conversacionales, o los que generan contenido sintético de audio, imagen, vídeo o texto, por ejemplo). La regulación se caracteriza básicamente por introducir un principio imperativo de información y transparencia.

Por último, figuran los sistemas de "riesgo mínimo", que son todos los demás. Incluyen la mayoría de las aplicaciones de IA actualmente disponibles en el mercado (videojuegos o filtros de *spam*, por ejemplo). No tienen regulación imperativa. De forma voluntaria, los proveedores de estos últimos sistemas pueden adoptar códigos de conducta para la aplicación voluntaria de requisitos específicos del Reglamento (art. 95 RIA).

A su vez, los sistemas y modelos de IA generativa (que en el RIA se denominan modelos y sistemas de IA de "uso general"), donde se incluyen ChatGPT, Bing Chat, Gemini o LlaMA, cuentan con una regulación *sui generis* articulada en un régimen de transparencia cualificado (arts. 51 y ss. RIA), así como en trasladar tímidamente algunos requisitos de los sistemas de IA de alto riesgo.

Así las cosas, el RIA establece normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en toda la UE (art. 1.2.a RIA). La norma europea pretende ofrecer un marco jurídico que garantice que los sistemas de IA son fiables

y respetan los derechos fundamentales de la persona.

Ahora bien, no se trata, ni mucho menos, de una norma que regule de forma integral y completa todas las cuestiones jurídicas relacionadas con la IA. Por ejemplo, deja fuera de su regulación materias tan importantes como la responsabilidad civil, la cual se podría haber integrado perfectamente en este Reglamento. Y lo mismo ocurre con la vertiente muy relevante de su conexión con el derecho de autor en materia de programas de ordenador, o con las cuestiones de propiedad intelectual respecto a los contenidos que la IA generativa ofrece al usuario final, que se apuntan tímidamente, pero que no se abordan, como hubiera sido lo deseable en un instrumento normativo de estas características.

El RIA sigue, como hemos dicho, un planteamiento basado en el riesgo. Por eso, la intensidad regulatoria que incorpora está adaptada al nivel de riesgo del concreto sistema de IA sobre la salud, la seguridad y los derechos fundamentales del usuario. De este modo, el grueso de la regulación está destinada a los señalados sistemas de "alto riesgo", que deben seguir procedimientos horizontales específicos de evaluación de la conformidad para certificar que cumplen los requisitos esenciales. Desde el punto de vista jurídico, esto añade una capa de elevada complejidad, ya que los dispositivos enriquecidos con IA también pueden estar sujetos a normas de seguridad de los productos para sus componentes. El concepto de "requisitos esenciales" es así crucial en la normativa de la UE sobre seguridad de los productos.

En efecto, con el llamado Nuevo Enfoque, introducido en los años 80, la normativa europea sobre seguridad de los productos pretendía establecer únicamente "requisitos esenciales", dejando los detalles técnicos a las "normas armonizadas" europeas. Este sistema se diseñó para eliminar las barreras comerciales derivadas de la diversidad de normas técnicas de las autoridades nacionales. La acreditación, al igual que el "marcado CE" y los procedimientos de conformidad, permitía que los productos conformes con las normas armonizadas se comercializaran libremente en el mercado interior en régimen de reconocimiento mutuo. Este marco se renovó considerablemente en 2008 con el denominado Nuevo Marco Legislativo (NML), que pretende ofrecer mejores mecanismos de gobernanza y reforzar el sistema europeo de vigilancia del mercado. Desde entonces, el paradigma regulatorio del NML se ha utilizado para regular diversos sectores, desde los juguetes hasta los productos sanitarios.

Con este planteamiento, el RIA pretende compatibilizar sus normas sobre IA con las de seguridad de los productos para evitar posibles duplicaciones. Su objetivo es abordar los riesgos específicos de seguridad de los sistemas de IA utilizando las normas contenidas en el nuevo instrumento normativo. En cambio, el Reglamento delega la seguridad general del producto final y sus requisitos específicos relativos a la integración segura de un sistema de IA en el producto final en la legislación pertinente en el marco del NML. Como resultado, la sección 2 del capítulo III del RIA contiene requisitos obligatorios esenciales ex ante para el diseño y desarrollo de sistemas de IA de "alto riesgo" y la especificación de estos requisitos tendrá lugar a través de "normas armonizadas" elaboradas por los organismos europeos de normalización: CEN, CENELEC y ETSI. Estas normas armonizadas regularán los detalles técnicos que el RIA deja sin especificar, proporcionando a los fabricantes una vía clara y jurídicamente segura para su cumplimiento. Además, este modelo regulatorio pone de relieve el papel estratégico de estas organizaciones a la hora de definir los aspectos sustantivos de la gobernanza de la IA en la UE como correguladores, tal y como han señalado los profesores Álvarez García y Tahirí Moreno (24).

En síntesis, el RIA, adoptando el marco establecido por el NML, promueve un nuevo modelo de gobernanza para la inteligencia artificial. Un elemento central de este modelo es la noción de que el cumplimiento de los requisitos esenciales de los sistemas de IA de "alto riesgo" se evaluará mediante evaluaciones de conformidad. Este enfoque distribuye la responsabilidad de la evaluación de la conformidad entre los propios proveedores o fabricantes, responsables del despliegue e importadores (arts. 16 y 23 RIA).

Como hemos apuntado, el RIA incluye una serie de obligaciones en sus requisitos esenciales

para los sistemas de IA de "alto riesgo". Se trata en esencia de la gestión de riesgos, la gobernanza de los datos, la transparencia, la supervisión humana y las medidas para garantizar la precisión, la solidez y la ciberseguridad de tales sistemas. Los requisitos de gestión de riesgos no son nuevos y se encuentran en otras normas (25) sobre seguridad de los productos. El Reglamento también exige el cumplimiento de una serie de criterios de calidad en el uso de datos de entrenamiento (art. 10 RIA). Así, los criterios del Reglamento imponen que los datos utilizados en el entrenamiento, validación y prueba sean pertinentes, representativos, sin errores y completos (art. 10 RIA). Se trata de una medida esencial para minimizar usos discriminatorios de la IA.

Otro aspecto cubierto por el Reglamento es la necesidad de elaborar una documentación técnica para demostrar el cumplimiento (art. 11 RIA). El procedimiento para crear esta documentación está armonizado dentro del propio Reglamento en su anexo IV. Esta documentación tiene por objeto proporcionar a las autoridades nacionales de supervisión y a los organismos notificados la información pertinente para evaluar el cumplimiento. Además, los sistemas de IA de "alto riesgo" deben estar diseñados para permitir el registro automático de acontecimientos o eventos (los llamados archivos *log* en inglés) con fines de trazabilidad (art. 12 RIA). El funcionamiento de los sistemas de IA debe ser lo suficientemente transparente como para garantizar que los usuarios —que la versión final del RIA denomina "responsables del despliegue"— puedan utilizar el sistema correctamente y comprender todas sus capacidades y limitaciones (art. 13 RIA).

Además, los fabricantes deben incorporar herramientas de interfaz persona-máquina en el diseño y desarrollo de los sistemas de IA de "alto riesgo" para permitir una supervisión eficaz por parte de personas físicas (art. 14 RIA). Esta supervisión por diseño debe permitir una comprensión completa de las capacidades y limitaciones del sistema, y posibilitar al usuario anular o detener el funcionamiento del sistema cuando sea necesario. Por último, el Reglamento exige que los proveedores diseñen sistemas de IA de "alto riesgo" precisos, sólidos y ciberseguros (art. 15 RIA). Esto incluye el diseño de sistemas resistentes, la creación de planes de copias de seguridad y medidas de mitigación, así como soluciones técnicas para evitar alteraciones no autorizadas.

Y es que el NML está diseñado para simplificar el proceso de cumplimiento normativo reduciendo las cargas financieras y logísticas que podrían surgir si los fabricantes tuvieran que demostrar el cumplimiento de unos requisitos esenciales ampliamente definidos. Teniendo esto en cuenta, se anima a los fabricantes a seguir normas técnicas ya establecidas, armonizadas y que hayan sido publicadas oficialmente en el DOUE, toda vez que el RIA establece una presunción de conformidad para los sistemas de IA de "alto riesgo" si se ajustan a las normas armonizadas. Aunque en principio el cumplimiento de estas normas es voluntario, lo que significa que los proveedores de IA también pueden elegir otras vías para demostrar la conformidad, en la práctica lo más probable es que los fabricantes y proveedores sigan las normas armonizadas para garantizar la conformidad. Una vez que la evaluación demuestre el cumplimiento de los requisitos esenciales establecidos en el RIA, los proveedores redactarán una declaración de conformidad y colocarán el "marcado CE" en el producto (art. 48 RIA). Seguir estas normas armonizadas ofrece a los fabricantes y proveedores cierto grado de seguridad jurídica. Esta seguridad se deriva del hecho de que estas normas son, en sí mismas, actos jurídicos de la Unión y pueden ser enjuiciadas por el TJUE. Por tanto, su cumplimiento equivale al cumplimiento de la regulación (art. 40 RIA). Por ello, los fabricantes y proveedores podrían inclinarse por estas normas, especialmente cuando se trate de sistemas de IA de "alto riesgo".

A la postre, las normas armonizadas proporcionarán *de facto* y también *de iure* las especificaciones sustantivas que deberán cumplir los sistemas de IA de "alto riesgo", toda vez que su aplicación permite al proveedor beneficiarse de la presunción de conformidad con los requisitos esenciales del RIA. Por todo ello, los organismos europeos de normalización desempeñan un papel fundamental a este

respecto. Son responsables del desarrollo de las normas armonizadas, que proveerán las especificaciones técnicas detalladas para los requisitos esenciales establecidos en el RIA. Por lo tanto, aunque el Reglamento establece la configuración reguladora general del modelo de gobernanza de la IA, los organismos europeos de normalización son quienes se encargarán del contenido real de la regulación del mercado de la IA en la UE. Y la Comisión Europea desempeña asimismo un papel cardinal, que podemos condensar en tres vertientes. En primer lugar, formula el mandato o petición a los organismos europeos de normalización para que elaboren estas normas. En segundo lugar, asesora a los mismos. Y, en tercer lugar, la Comisión Europea recepciona y da su conformidad a la norma armonizada antes de proceder a su publicación en el DOUE.

En consecuencia, el hecho de que el RIA utilice el paradigma regulatorio de la seguridad de los productos suscita multitud de interrogantes. De todos ellos quiero destacar dos. En primer lugar, cabe preguntarse si una técnica de armonización que se desarrolla en el mundo físico puede transponerse tan fácilmente a un entorno en línea y al ámbito de la IA, pues son muy notorias las diferencias entre una lavadora, un coche autónomo o un sistema de IA que determina la concesión de un préstamo, por ejemplo. En segundo lugar, el NML ha sido criticado con frecuencia por su falta de legitimación democrática y de responsabilidad y, en relación con esto, por la falta de participación pública y de supervisión pública en los procesos de normalización y certificación.

Así las cosas, la regulación jurídica de la IA no es una tarea fácil dada la evolución fotónica que estamos viviendo tras el *tsunami* provocado por ChatGPT y otros sistemas de IA generativa. Con la inevitable inestabilidad normativa y técnica, es difícil predecir lo que nos deparará el futuro. Podemos afirmar que el uso de la IA en diferentes sectores requiere diferentes enfoques y estrategias de regulación, que incluyen una legislación experimental que pueda surgir en el marco de los espacios controlados de pruebas o *sandboxes* (art. 57 RIA), mecanismos para actualizaciones legislativas proactivas y una legislación que permita modulaciones y excepciones.

8.5. ESPECIAL INCIDENCIA EN LOS DERECHOS DE LOS CIUDADANOS

Uno de los caballos de batalla en la elaboración del RIA ha sido, precisamente, el alcance de los derechos de los ciudadanos. El texto finalmente aprobado contiene unos tímidos derechos en los artículos 85 y 86, y que pasamos a examinar.

8.5.1. El derecho a presentar una reclamación ante una autoridad de vigilancia del mercado

El artículo 85 del RIA, en su primer párrafo, abre la posibilidad de presentar una "reclamación" con base en la infracción de disposiciones del Reglamento a cualquier persona física o jurídica que tenga motivos para pensar que se haya cometido alguna vulneración. Aunque esta norma recuerda al mecanismo arbitrado en el artículo 77 del RGPD, lo cierto es que en este último se le reconoce la posibilidad de dirigirse directamente a la autoridad de control competente en la materia (la Agencia Española de Protección de Datos, en el caso de España), lo que permite a este incoar por esta vía un auténtico procedimiento administrativo.

En cambio, el artículo 85.1 del RIA no exige al sujeto legitimado verse directamente afectado o concernido por ello, a pesar de que el término "reclamación" invite a pensar en este sentido. Así, como señala Castilla Barea (24), el reclamante puede ser tanto un sujeto que se haya sentido directamente perjudicado por la infracción que denuncia, como alguien que actúe movido por cualquier otro interés legítimo, como podría

ser el caso, por ejemplo, de una asociación de consumidores, una persona experta del ámbito académico, etc.

Obviamente, precisa además el párrafo primero del precepto que esta legitimación es independiente de la que pudiera corresponder a esas mismas personas físicas o jurídicas en cualquier otro ámbito administrativo o judicial, lo que lógicamente sí apunta en la dirección de que el reclamante pueda ser un sujeto directamente concernido por la infracción que pone de manifiesto mediante la indicada reclamación.

Por su parte, la remisión que efectúa el párrafo segundo del precepto al Reglamento (UE) 2019/1020 (27) para establecer el efecto de tales reclamaciones y el procedimiento por el que habrán de tramitarse, conduce: de un lado, al art. 11.3.d) RVM, que llama a las autoridades de vigilancia del mercado a tomar en cuenta, a la hora de decidir qué comprobaciones realizar, "las reclamaciones de los consumidores y otra información recibida de otras autoridades, operadores económicos, medios de comunicación y otras fuentes que puedan indicar incumplimiento"; y, de otro, al art. 11.7.a) RVM, que encomienda a las autoridades de vigilancia del mercado el establecimiento de los procedimientos para el seguimiento de las reclamaciones o informes sobre cuestiones relativas a incumplimientos. Por tanto, compete a las autoridades nacionales competentes en cada caso establecer tales procedimientos.

8.5.2. El derecho a explicación de decisiones tomadas individualmente

A diferencia del anterior, el derecho reconocido en el artículo 86 del RIA sí se restringe a aquellas personas que se hayan visto afectadas o perjudicadas por la decisión acerca de la cual se le permite pedir explicaciones. Como precisa Castilla Barea (26), el sujeto legitimado "ha de ser, además, una persona física lo que, a pesar del silencio de la norma al respecto, se infiere de la referencia a su salud, seguridad o derechos fundamentales". Los elementos cuya concurrencia exige la norma para que dicha persona pueda ejercer el derecho que en ella se le reconoce son los siguientes:

1. Que el responsable del despliegue de un sistema de IA de alto riesgo que figure en el anexo III, con la excepción de los mencionados en su punto 2 —que son los relativos a las infraestructuras críticas—, haya tomado una decisión basándose en los resultados de salida de uno de estos sistemas.
2. Que dicha decisión produzca efectos jurídicos para la persona afectada "o le afecte considerablemente del mismo modo" en un sentido negativo o perjudicial para su salud, seguridad o derechos fundamentales. Siguiendo a Castilla Barea, entendemos que el legislador se refiere a aquellas decisiones que, proviniendo de responsables del despliegue que son sujetos privados, no producen en puridad efectos jurídicos sobre las personas afectadas por ellas, pero tienen una enorme trascendencia en su vida, como puede ser el caso, por ejemplo, de los sistemas que, de acuerdo con el anexo III, punto 5, letra c) del RIA, pueden determinar que se conceda o no un seguro de salud a una persona o se le exija para ello una prima exorbitada. El artículo 86 del RIA recuerda en este punto al artículo 22.1 del RGPD, precepto que también asiste en ciertos casos, modo y medida al interesado para conocer la lógica aplicada en la toma de decisiones automatizadas que le afecten (arts. 14.2.g) y 15.1.h) RGPD).
3. Por último, es preciso que el ejercicio de este derecho no esté excepcionado o restringido por otras normas del Derecho de la Unión o nacionales conformes con aquel, respecto de determinados sistemas de IA (art. 86.2 RIA).

La consecuencia es que dicha persona afectada pueda solicitar del responsable del despliegue explicaciones claras y significativas sobre el papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada.

Con todo, debe tenerse en cuenta que el derecho consignado en el artículo 86 del RIA

tiene carácter subsidiario de cualquier otra norma europea que reconozca un derecho similar en el contexto que le sea propio, como se desprende de su apartado 3 que lo condiciona a "que el derecho a que se refiere el apartado 1 no esté previsto de otro modo en el Derecho de la Unión".

8.6. CONCLUSIÓN

La inteligencia artificial genera un amplio abanico de beneficios económicos y sociales en todos los sectores y actividades. Su uso puede proporcionar ventajas competitivas esenciales a las empresas y administraciones públicas, y facilitar la obtención de resultados positivos desde el punto de vista social y ambiental en los ámbitos de la asistencia sanitaria, la agricultura, la educación y la formación, la gestión de infraestructuras, la energía, el transporte y la logística, los servicios públicos, la seguridad, la justicia, la eficiencia de los recursos y la energía, así como la mitigación del cambio climático y la adaptación al mismo.

También puede contribuir a mejorar la predicción, optimizar las operaciones y la asignación de los recursos, y a personalizar las soluciones digitales que se encuentran a disposición de la población y las organizaciones. Es, por tanto, necesario garantizar su buen gobierno con el fin de aprovechar todas las oportunidades que esta supertecnología ofrece, al tiempo que se asegura el control y la limitación de los riesgos derivados de un uso indebido.

El Reglamento (UE) 2024/1689 nace en el contexto de la Estrategia europea de inteligencia artificial de la Comisión Europea, a través de la cual se pretende convertir a la UE en una región de referencia mundial para la IA, garantizando que esta se centre en la persona humana y sea sostenible, segura, inclusiva y fiable, y que garantice el respeto a los derechos fundamentales, la democracia, el Estado de Derecho y la sostenibilidad medioambiental. Al mismo tiempo, el RIA tiene por objetivo impulsar la innovación y establecer a la UE como líder en el campo de la IA, actuando como un catalizador de la industria.

El RIA es una norma altamente compleja y con evidentes problemas de calidad normativa. A mi juicio, muchas de las críticas están justificadas. Sin embargo, no deben olvidarse los numerosos beneficios que la legislación recién aprobada pretende aportar para la integración europea. La seguridad de cara al futuro consiste en una legislación que sea eficaz y se adapte a pesar de los cambios jurídicos, sociales y técnicos que se produzcan con el tiempo. Solo el tiempo dirá si el RIA ha logrado anticiparse a estos retos y ha proporcionado los mecanismos adecuados para abordarlos.

Al menos, el Reglamento constituye un buen punto de partida en la creciente necesidad política de regular la IA en una amplia gama de ámbitos. Y corresponderá a los juristas participar en el proceso de implementación de sistemas de IA en la respectiva entidad para asegurar que los mismos no solo cumplen con el ordenamiento jurídico en vigor, sino que coadyuvan verdaderamente a la satisfacción de las necesidades reales de la organización en cuestión.

8.7. REFERENCIAS BIBLIOGRÁFICAS

1. Barrio M. Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet. Valencia: Tirant lo Blanch; 2018.
2. Barrio M. Los principios generales del Derecho de los Robots. En: Barrio M. (dir.) Derecho de los Robots. 2.ª ed. Madrid: Wolters Kluwer; 2019. p. 140 y ss.
3. Barrio M. Inteligencia artificial: origen, concepto, mito y realidad. El Cronista del Estado Social y Democrático de Derecho. 2022; (N° 100).

4. Barrio M. (dir.) El Reglamento Europeo de Inteligencia Artificial. Valencia: Tirant lo Blanch; 2024.

5. Barrio M. (dir.) Comentarios al Reglamento Europeo de Inteligencia Artificial. Madrid: La Ley; 2024.

6. Bommasani R, *et al*. On the opportunities and risks of foundation models. arXiv; 2022. Disponible en: https://doi.org/10.48550/arXiv.2108.07258

7. Barrio M. ChatGPT y su impacto en las profesiones jurídicas. Diario La Ley. 2023; (N° 10289.

8. Parlamento Europeo. Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)) [Internet]. Estrasburgo: Europa.eu; 2017. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html

9. Aransay A. Antecedentes y propuestas para la regulación jurídica de los robots. En: Barrio M. (dir.) Derecho de los Robots. 2.ª ed. Wolters Kluwer; 2019. p. 93-114.

10. Comisión Europea. Inteligencia artificial para Europa COM(2018)237 final [Internet]. Bruselas: digital-strategy.ec.europa.eu; 2018. Disponible en: https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe

11. Comisión Europea. Plan Coordinado sobre Inteligencia Artificial COM(2018)795 final [Internet]. digital-strategy.ec.europa.eu; 2018. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/plan-ai

12. Comisión Europea. Libro Blanco sobre la Inteligencia Artificial: un enfoque europeo hacia la excelencia y la confianza COM(2020)65 final [Internet]. Bruselas: eur-lex.europa.eu; 2020. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0065

13. Parlamento Europeo. Régimen de responsabilidad civil de la inteligencia artificial 2020/2014(INL) [Internet]. oeil.secure.europarl.europa.eu; 2020. Disponible en: https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1636987

14. Parlamento Europeo. Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos - Considerando 9 (DO L 210 de 7.8.1985, p. 29) [Internet]. 2020. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_ES.html#ref_2_3

15. Comisión Europea. Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la Responsabilidad por Productos Defectuosos COM(2022)495 final [Internet]. Bruselas: eur-lex.europa.eu; 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0495

16. Comisión Europea. Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad por IA) COM(2022)496 final [Internet]. Bruselas: eur-lex.europa.eu; 2022. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0496

17. Comisión Europea. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión COM(2021)206 final [Internet]. Bruselas: eur-lex.europa.eu; 2021. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

18. Barrio M. Manual de Derecho digital. 4.ª edición ampliada y actualizada. Valencia: Tirant lo Blanch; 2025.

19. Parlamento Europeo. 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 datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [Internet]. 2016 abr 27. Disponible en: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

20. Parlamento Europeo. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) [Internet]. 2022 oct 19. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32022R2065

21. Parlamento Europeo. Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) [Internet]. 2022 oct 12. Disponible en: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

22. Parlamento Europeo. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) [Internet]. Disponible en: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=es

23. Barrio M. Sobre la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Diario La Ley. 2023; (N° 10349).

24. Álvarez V, Tahirí J. La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque. Rev Gen Derecho Adm. 2023;(N° 63).

25. Parlamento Europeo. Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos (Texto pertinente a efectos del EEE) [Internet]. 2001. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32001L0095

26. Castilla M. Vigilancia postcomercialización, códigos de conducta y directrices. En: Barrio M. (dir.). El Reglamento Europeo de Inteligencia Artificial. Valencia: Tirant lo Blanch; 2024.

27. Parlamento Europeo. Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.° 765/2008 y (UE) n.° 305/2011 (RVM en lo sucesivo) [Internet]. 2019. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2019.169.01.0001.01.SPA

PROYECTO EUTELIS | CÁTEDRA JEAN MONNET

La ambición de este libro es ser una fuente rigurosa de información para especialistas, legisladores y profesionales del sector y, al mismo tiempo, ofrecer una guía reflexiva e inspiradora para quienes se interesan por el futuro digital de Europa.

En un momento donde las decisiones tecnológicas son también decisiones políticas, creemos que este trabajo contribuye a entender los dilemas, riesgos y oportunidades que marcarán el rumbo de una Europa que quiere seguir siendo relevante, justa y soberana en el siglo XXI.

Miguel López-Coronado Sánchez-Fortún
Jorge Pérez Martínez

Cofinanciado por la Unión Europea

Cátedra Jean Monnet > EUTELIS

Universidad Europea del Atlántico