digitales_

Resumen contenido dossieres legislativos UE

LT regulación entorno digital

Marzo 2022

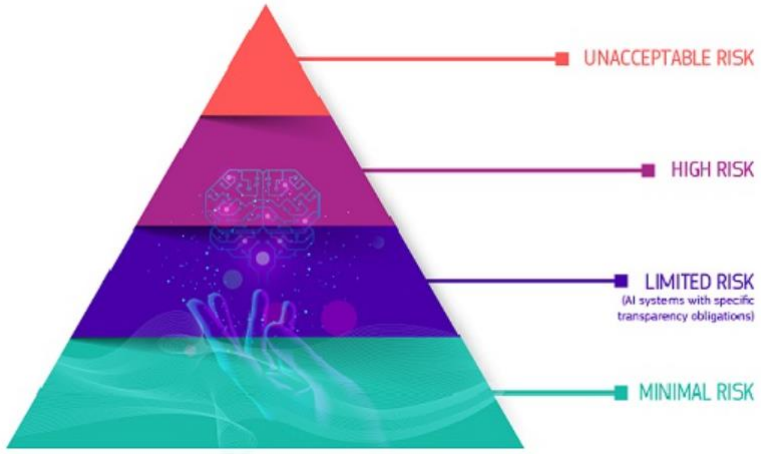
Reglamento IA

- *Comisión Europea: 21/04/21 Adopción de la propuesta de Reglamento COM(2021) 206 final- Responsable:* ***Thierry Breton,*** *comisario europeo de Mercado Interior.*
- *Parlamento Europeo: Comisión Responsable: Mercado Interior y Protección del Consumidor (IMCO). - Ponente:* ***Brando Benifei (Italia, S&D****). En la sombra: Deirdre Clune (Irlanda, PPE), Svenja Hahn (Alemania, RE), Kim van Sparrentak (Países Bajos, Verdes/ALE), Katerina Konecna (Chequia, GUE/NGL).*

Propuesta de 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

Ámbito de aplicación

subjetivo y territorial amplio que comprendería a todos los actores dentro de la cadena de valor de la IA (es decir, proveedores, importadores, distribuidores) y alcanzaría tanto aquellos ubicados en la UE como los empleados en un tercer país, (siempre y cuando, en este último caso, desplieguen los efectos en la UE).



The European Union's draft AI regulations classify AI systems into three risk categories.

Unacceptable-risk AI systems	High-risk AI systems	Limited- and minimal-risk AI systems
• Subliminal, manipulative, or exploitative techniques causing harm • Real-time, remote biometric identification systems used in public spaces for law enforcement • All forms of social scoring	• Systems that evaluate consumer creditworthiness • Recruiting or employee-management systems • Systems utilizing biometric identification in nonpublic spaces • Safety-critical systems (eg, systems that would put the health of citizens at risk due to failure) • Any systems used in the administration of justice	• AI chatbots • AI-enabled video and computer games • Spam filters • Inventory-management systems • Customer- and market-segmentation systems • Most other AI systems

Reglamento IA

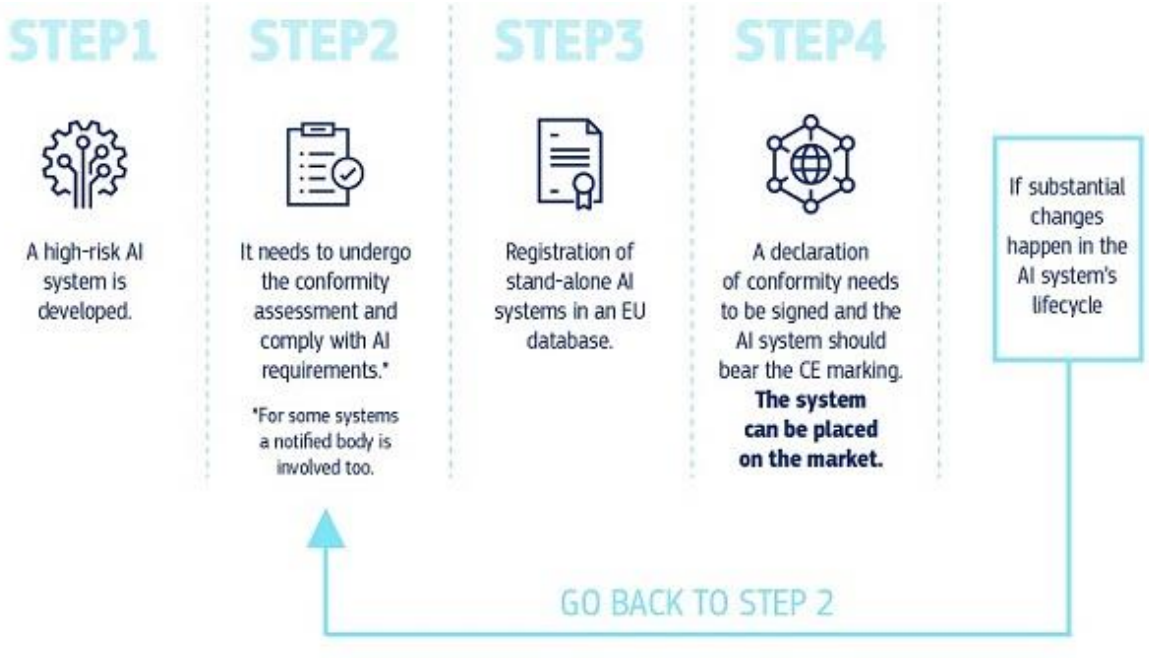
digitales_

Clasificación	Obligaciones
1. Sistemas de IA prohibidos. • serie de sistemas de IA, listados de forma tasada y periódicamente revisados, cuyo uso estaría prohibido por implicar un riesgo inadmisible para la seguridad, la vida y los derechos fundamentales. • Dicho listado incluye sistemas **capaces de manipular el comportamiento humano, predecir información respecto a colectivos o grupos para identificar sus vulnerabilidades o circunstancias especiales, o aquellos que impliquen la identificación biométrica o la videovigilancia masiva en directo por parte de las autoridades en espacios públicos.**	➢ Estos sistemas implican de partida un riesgo inadmisible y por tanto están prohibidos . ➢ No obstante, y en particular, los consistentes en **sistemas de identificación biométrica en remoto y en tiempo real en espacios públicos, se permitirían excepcionalmente para el cumplimiento de la ley y, en este caso, bajo autorización judicial o administrativa.** ➢ Dicha autorización podría ser solicitada con posterioridad a su implementación en casos de "extrema urgencia", cuestión que ha suscitado un gran debate

2 . Sistemas de IA de alto riesgo.
• si bien no están prohibidos, suponen un "alto riesgo" para los derechos y libertades de los individuos y, por consiguiente, deben estar sujetos a ciertas obligaciones reforzadas que garanticen su uso legal, ético, robusto y seguro.
  • **Infraestructuras críticas** (por ejemplo, transporte)
  • **Formación educativa o vocacional** , (por ejemplo, calificación de exámenes);
  • **Componentes de seguridad de los productos** (por ejemplo, aplicación de IA en cirugía asistida por robot);
  • **Empleo, gestión de trabajadores y acceso al autoempleo** (por ejemplo, software de clasificación de CV para procedimientos de contratación);
  • **Servicios públicos y privados esenciales** (p. ej., calificación crediticia que niega a los ciudadanos la oportunidad de obtener un préstamo);
  • **Cumplimiento de la ley que pueda interferir con los derechos fundamentales de las personas** (por ejemplo, evaluación de la confiabilidad de la evidencia);
  • **Gestión de la migración, el asilo y el control de fronteras** (por ejemplo, verificación de la autenticidad de los documentos de viaje);
  • **Administración de justicia y procesos democráticos** (por ejemplo, aplicación de la ley a un conjunto concreto de hechos).
	Podrían permitirse siempre y cuando sean sometidos a una evaluación de conformidad y gestión del riesgo que suponen durante toda su vida útil. Cada operador de la cadena de valor estaría sometido a una serie de **obligaciones específicas**
	➢ **Gobernanza de datos**: que los datos empleados revistan ciertos estándares de calidad, supervisión examinación de sesgos, etc.
	➢ **Seguridad y supervisión humana:** En última instancia siempre tendrá que haber una persona con capacidad de control para mitigar eventuales riesgos.
	➢ **Deberes de transparencia**: es decir, que se describan las características del funcionamiento del sistema y la identidad y datos del proveedor.
	➢ **Inscripción en una base de datos a nivel europeo:** La inscripción deberá llevarse a cabo con carácter previo a la puesta a disposición en el mercado.
	➢ **Superación del test de conformidad y obtención de la certificación correspondiente:** Serán aprobadas especificaciones técnicas con las que habrá que cumplir.

Reglamento IA

Clasificación	Obligaciones
3. **Sistemas de IA de riesgo medio/bajo.** • Sistemas que no suponen un alto riesgo para los derechos y libertades • Incluyen determinadas tecnologías de menor sofisticación o capacidad de intrusión tales como asistentes virtuales o chatbots	Únicamente estarían sometidos a un conjunto de normas de transparencia dirigidas a garantizar que su funcionamiento y características son conocidos por los usuarios
4. **Resto de sistemas de IA.** • No estarían sujetos a ninguna obligación en particular, pudiendo los agentes de la cadena elegir si desean adherirse a sistemas voluntarios de cumplimiento. • estos sistemas quedarían, en principio, fuera del ámbito de aplicación del reglamento.	De mantenerse la redacción propuesta, estos sistemas estarían sujetos a sistemas voluntarios de autorregulación, como la adhesión a códigos de conducta voluntarios. Esta propuesta de dejar abierta la regulación de los sistemas comprendidos en esta categoría está siendo objeto de discrepancia por parte de sectores que abogan por una mayor regulación, incluso en el caso de sistemas de menor sofisticación y que actualmente representan el gran bloque de sistemas existentes en el mercado.



•Incumplimiento relativo a prácticas prohibidas y las obligaciones de gobernanza de datos de los sistemas de IA de alto riesgo: hasta 30 millones de euros o el 6% del volumen de negocio anual total a escala mundial del ejercicio financiero anterior;

•Incumplimiento de cualquier otro requisito u obligación: hasta 20 millones de euros o el 4% del volumen de negocio anual total a escala mundial del ejercicio financiero anterior;

•Suministro de información incorrecta, incompleta o engañosa a los organismos y/o autoridades nacionales: hasta 10 millones de euros o el 2% del volumen de negocio anual total a escala mundial del ejercicio financiero anterior.

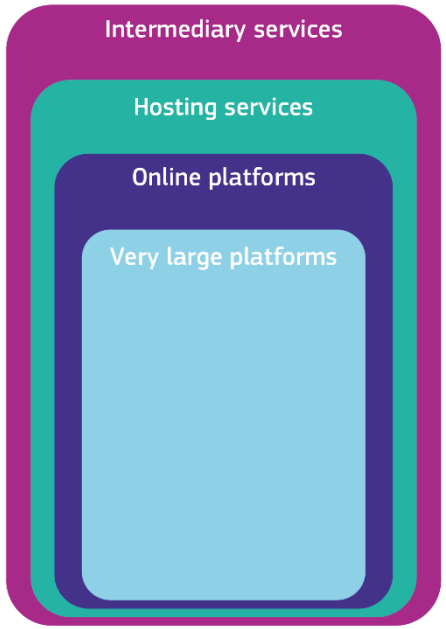
Ley de servicios digitales (Digital Service Act) – *contenido y servicios ilegales*

digitales_

[Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC]

A quien afecta

- Servicios de intermediación
- Servicios de alojamiento web/nube
- Plataformas online
- Grandes plataformas online



Nuevas obligaciones

Responsabilidad prestadores de servicios digitales:

i. procesos específicos para solicitar la retirada de contenidos ilícitos
ii. mecanismos para permitir que los usuarios puedan defenderse en caso de que entiendan que sus contenidos han sido retirados sin justificación
iii. obligación de cooperar con las autoridades de los Estados Miembros tanto en la retirada de contenidos ilícitos como en la identificación de determinados usuarios.

Obligación de diligencia debida:

(i) Establecer punto de contacto único;
(ii) designar un **representante legal**
(iii) describir las políticas, procedimientos y medidas que emplean a la hora de moderar contenidos, incluyendo el uso de **sistemas algorítmicos para la toma de decisiones;**
(iv) publicar **información relativa a las solicitudes de retirada de contenidos ilícitos recibidas de terceros** (e.g. autoridades públicas, ciudadanos) o fruto de su propia actividad de monitorización voluntaria.

	Servicios de intermediación	Servicios de alojamiento	Plataformas online	Grandes plataformas online
Informes de transparencia	X	X	X	X
Requisitos relativos a la protección de los derechos fundamentales	X	X	X	X
Cooperación con las autoridades nacionales en materia de órdenes judiciales y administrativas	X	X	X	X
Puntos de contacto y representante legal	X	X	X	X
Mecanismos de notificación y acción e información a los usuarios (N&A)		X	X	X
Mecanismos de reclamación en procesos de N&A			X	X
Informadores de Confianza (*trusted flaggers*)			X	X
Medidas contra notificaciones y contra-notificaciones abusivas			X	X
Verificación de terceros vendedores ("KYBC")			X	X
Transparencia de la publicidad frente al usuario			X	X
Denuncia de delitos			X	X
Análisis y riesgos y responsable de cumplimiento				X
Auditorías internas				X
Transparencia en los sistemas de recomendación				X
Compartir datos con las autoridades públicas				X
Códigos de conducta				X
Cooperación en crisis				X

Ley de mercados digitales (Digital Market Act) – *grandes plataformas*

digitales_

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)

A quien afecta - grandes plataformas

- ❑ posición económica fuerte, un impacto significativo en el mercado interior y actividades en muchos países de la UE

(*ingresos al menos 6.500 millones en los tres últimos años o una capitalización media de al menos 65.000 millones de dólares en el último ejercicio fiscal. Además, debe proveer uno de estos servicios clave en al menos tres estados miembros.)*

- ❑ sólida posición de intermediadora

(servicio con más de 45 millones de usuarios activos mensuales y con más de 10.000 usuarios empresariales activos anuales)

- ❑ que disfruten de una posición consolidada en el mercado.

si se cumplen los dos anteriores requisitos en cada uno de los últimos tres ejercicios

motores de búsqueda, redes sociales, *marketplaces*, *app store*, otros servicios de intermediación *online*, ciertos servicios de mensajería instantánea, servicios en la nube, plataformas de intercambio de videos, sistemas operativos y servicios de publicidad en al menos tres Estados miembros de la Unión Europea.

	Black-list	Grey-list
Transparency in ad intermediation	- Transparency on price for advertisers and publishers (art.5.g)	- Transparency on performance for advertisers and publishers (6.1g)
Envelopment through bundling or self-preferencing Access platforms and data	- Bundling CPS with ID services (5.e) - Bundling CPSs for which gatekeeper designation apply (5.f)	- Rely on business users' data in dual role setting (6.1a) - App un-installing (art.6.1b) - Discriminatory ranking (6.1d) - Side loading: interoperability with third-party apps and app stores (6.1c) - Business users free of charge access to real-time, data (art.6.1i) - Sharing search data (art.6.1j)
End-users and business users mobility	- MFN/parity clause (5b) - Anti-steering clause (5c)	- Device neutrality: Prohibition of restricting user apps and services switching on an OS (6.1e) - Access and interoperability for business users and providers of ancillary services to OS and other features (6.1f) - Obligation real-time data portability for business users and end-users (6.1h)
Unfair sensu stricto	- Data fusion/lakes without users choices (5.a) - Preventing complaints to authorities (art.5d)	- FRAND access to app stores (6.1k)

Ejemplo de lo que deberán hacer: las plataformas guardianas de acceso deberán

- Habrá situaciones concretas en que los guardianes de acceso deben permitir a terceros interactuar con sus propios servicios.
- permitir que sus empresas usuarias accedan a los datos que generan al utilizar la plataforma del guardián de acceso
- ofrecer a las empresas que publicitan en su plataforma las herramientas y la información necesarias para que anunciantes y editores lleven a cabo su propia verificación independiente de los anuncios alojados por el guardián de acceso
- permitir que sus empresas usuarias promocionen sus ofertas y celebren contratos con sus clientes fuera de la plataforma del guardián de acceso

Ejemplo de lo que no podrán hacer: las plataformas guardianas de acceso ya no podrán

- clasificar más favorablemente sus propios servicios y productos que productos o servicios similares ofrecidos por terceros a través de la plataforma del guardián de acceso
- impedir que los consumidores se pongan en contacto con las empresas fuera de la plataforma del guardián de acceso
- impedir que los usuarios desinstalen programas o aplicaciones preinstaladas si así lo desean.

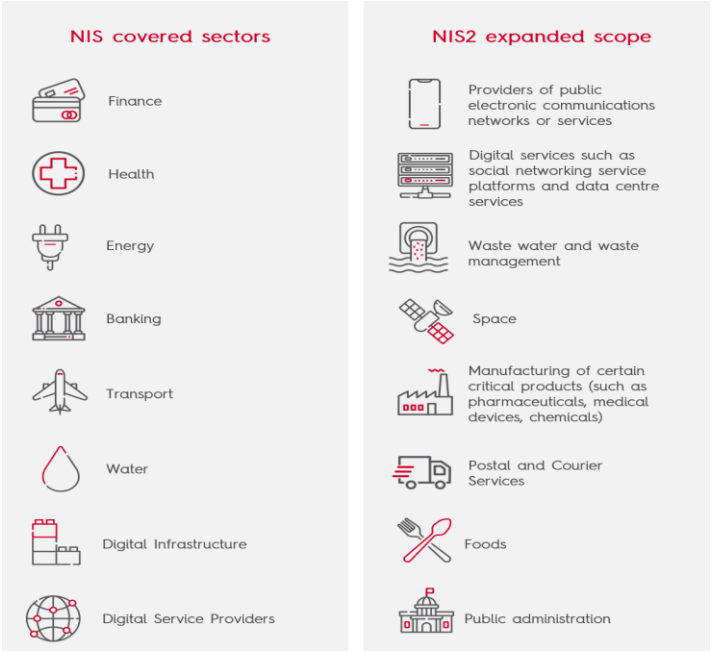
NIS2 - Directiva europea de ciberseguridad

Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148

NOVEDADES

(i) La ampliación del ámbito de aplicación de la nueva Directiva NIS 2, a través de dos vías:

- La ampliación del concepto entidades esenciales: habiéndose introducido dentro del mismo sectores o actores previamente no previstos en la anterior Directiva NIS, como por ejemplo energía, transportes, banca, infraestructuras de los mercados financieros, sanidad, agua potable, aguas residuales, infraestructura digital, administración pública y sector espacial.
- La introducción de un nuevo concepto denominado entidades de "sectores importantes": si bien el Anexo incluyendo la enumeración exhaustiva de las entidades que serán consideradas como pertenecientes a "sectores importantes" aún no ha sido publicado, en la exposición de motivos del texto publicado se avanza que estos sectores incluirán, entre otros: servicios postales y de mensajería, gestión de residuos, fabricación, producción y distribución de sustancias y mezclas químicas, producción, transformación y distribución de alimentos, fabricación y proveedores de servicios digitales



(ii) nuevo foco de interés para la regulación de la ciberseguridad centrado en las asociaciones público-privadas La nueva versión de la Directiva NIS 2 plantea la creación de PPPs especializados en ciberseguridad para el desarrollo de las estrategias nacionales en materia de ciberseguridad de los estados miembros (los "**EEMM**").

(iii) importancia de armonizar la normativa que regula la prevención, detección y respuesta a las ciberamenazas y ciberataques. Para ello, se impone a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) la responsabilidad de proveer a los EEMM y las autoridades competentes la orientación para que adapten sus estrategias nacionales de ciberseguridad vigentes a los requisitos y obligaciones establecidos en la Directiva.

(iv) En lo relativo a los nuevos requisitos de seguridad **exigidos se incluyen, entre otros, la respuesta a incidentes, la seguridad de la cadena de suministro, el cifrado y la divulgación de vulnerabilidades.**

(v) Asimismo, la ciberseguridad pasaría a ser responsabilidad de los altos directivos, mientras que, por otro lado, los EEMM podrían identificar a las entidades más pequeñas con un perfil de alto riesgo para la seguridad.

(vi) Se propone una definición de "riesgo" entendida como el *potencial de pérdida o perturbación causado por un incidente, que debe expresarse como una combinación de la magnitud de dicha pérdida o perturbación y la probabilidad de que se produzca dicho incidente*.

(vii) En cuanto materia de sanciones, seguirán siendo los EEMM los encargados de establecer el régimen sancionador aplicable, adoptando todas las medidas necesarias (efectivas, proporcionadas y disuasorias) para su ejecución.

Estrategia europea de datos

Data Governance Act – *Ley Gobernanza de datos*

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)

crea los procesos y estructuras para facilitar el intercambio de datos por parte de las empresas, los particulares y el sector público

La gobernanza de los datos se refiere a un **conjunto de normas y medios para utilizarlo**s, por ejemplo a través de mecanismos de intercambio, acuerdos y normas técnicas.

Implica estructuras y procesos para compartir datos de manera segura, incluso a través de terceros de confianza.

1 . **Hacer disponibles los datos del sector público**
2. **Intercambio de datos entre empresas**, a cambio de remuneración en cualquiera de sus formas.
3, Permitir el **uso y transferencia de datos** con motivos **altruistas**.
4. **Comité Europeo de Innovación** en materia de Datos

Data Act – *Ley Europea de Datos*

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

aclara quiénes pueden generar valor a partir de los datos y en qué condiciones

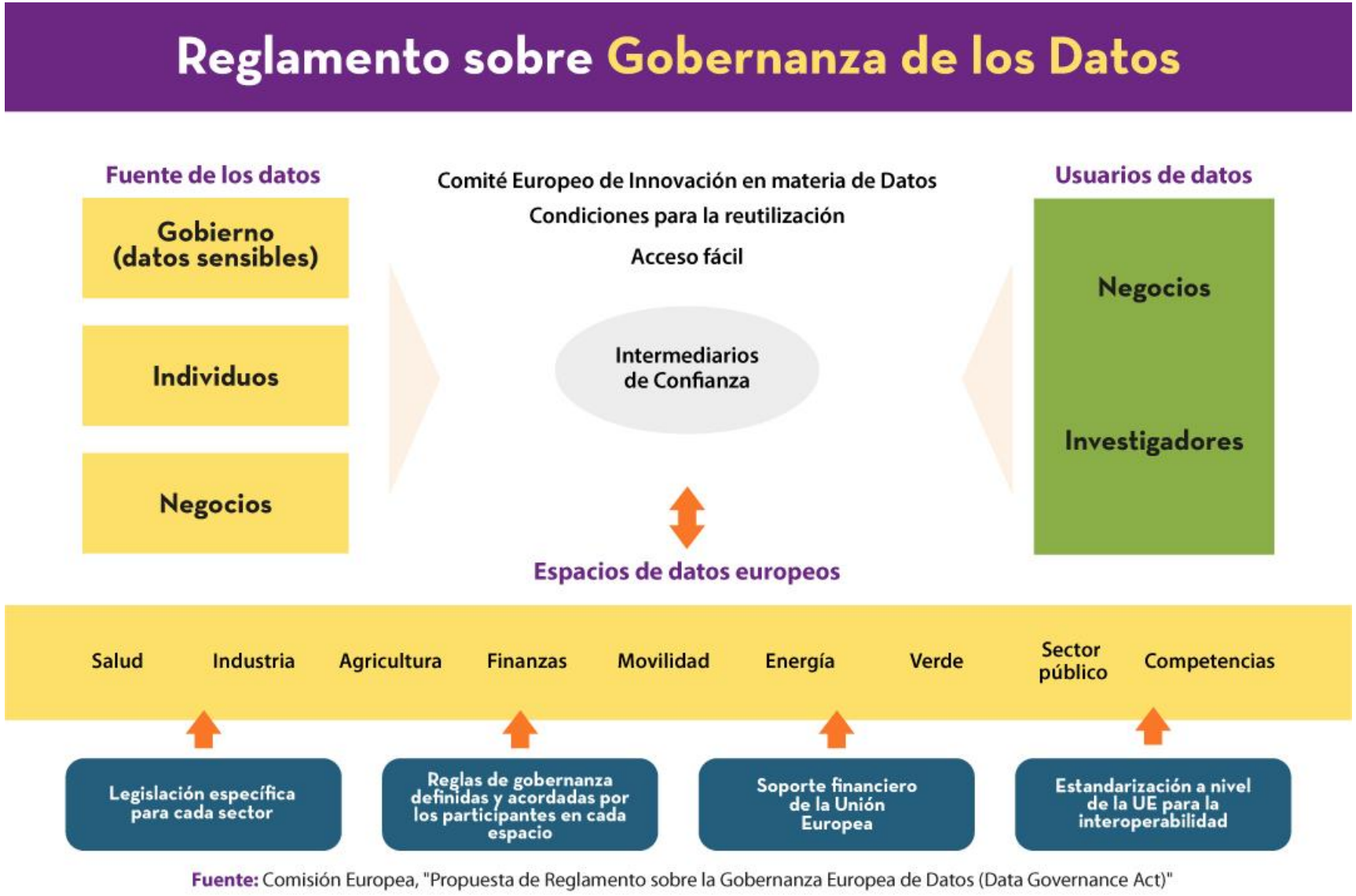
- Medidas que permitan a **los usuarios de dispositivos conectados acceder a los datos generados por ellos**, que suelen recoger exclusivamente los fabricantes, e intercambiarlos con terceros para prestar servicios de posventa u otros servicios innovadores basados en datos.
- Medidas para reequilibrar el **poder de negociación de las pymes** mediante la prevención del abuso de los desequilibrios contractuales.
- **Mediadas para que organismos del sector público obtengan y usen datos en poder del sector privado** que sean necesarios en circunstancias excepcionales
- normas que **permitan a los clientes cambiar efectivamente de proveedores de servicios de tratamiento de datos en la nube y establezcan salvaguardias contra la transferencia ilegal de datos**

Data Governance Act – *Ley Gobernanza de datos*

[Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)]

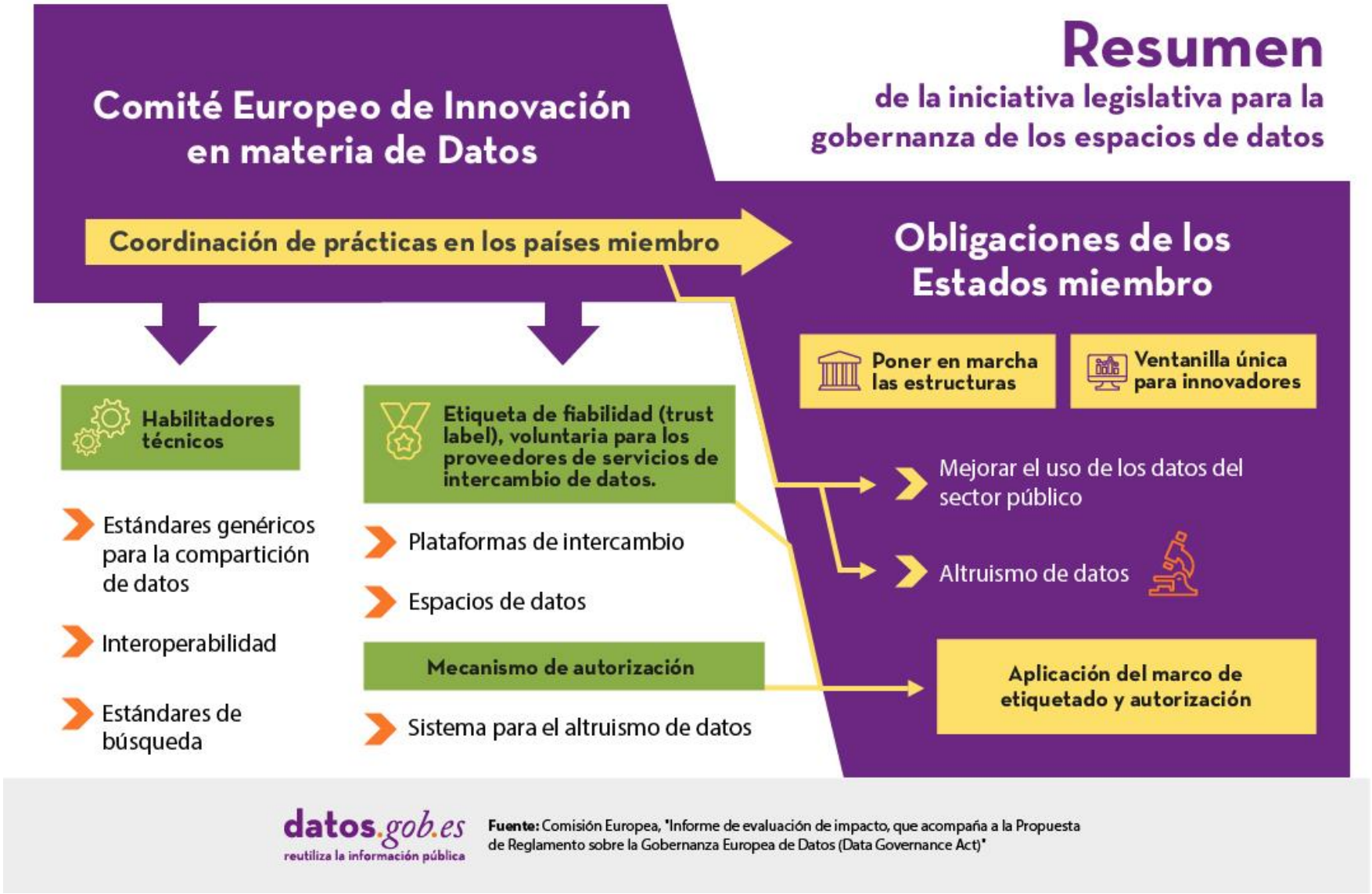
Objetivos

- Identificar mecanismos para mejorar la reutilización de datos del sector público
- Promover la confianza en los intermediarios
- Facilitar la cesión de datos con fines altruistas
- Impulsar los aspectos horizontales de la gobernanza



Fuente: Comisión Europea, "Propuesta de Reglamento sobre la Gobernanza Europea de Datos (Data Governance Act)"

Data Governance Act – *Ley Gobernanza de datos*



Data Act – *Ley Europea de Datos*

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

digitales_

Objetivo es aumentar el uso y el acceso a los datos, en particular los datos no personales regulados por la ley de contratos en situaciones B2B para garantizar la equidad en los mercados.

Antecedentes

- **Comunicación sobre una estrategia europea para los datos** adoptada por la Comisión Europea en febrero de 2020 destacó que se podrían emprender más acciones de la UE en una Ley de datos, entre otras cosas, para fomentar el intercambio de datos entre empresas y gobiernos para el interés público, apoyar a las empresas. el intercambio de datos entre empresas y evaluar el marco de los derechos de propiedad intelectual con miras a mejorar aún más el acceso y el uso de los datos.

- En **mayo de 2021, la Comisión publicó sus Evaluaciones de impacto inicia**l sobre la próxima Ley de datos.

- Presentada el 23 de febrero de 2022, busca incentivar la inversión en la generación y reutilización de los datos generados en la UE. En concreto, pretende optimizar la explotación del incremento masivo de datos generados tanto por humanos como por las máquinas, además de aumentar la confianza en materia de compartición de datos y superar las barreras que impiden una innovación

Contenido previsible para abordar la actual problemática relacionada

- **Intercambio de datos B2Government:** *las empresas no ponen suficientes datos a disposición de los servicios gubernamentales y optan por comercializarlos. Esto limita la capacidad de los gobiernos para crear sus propios modelos de datos en interés del público.*
- **Términos B2B injustos:** *los titulares de datos pueden imponer unilateralmente términos y condiciones injustos a otras empresas que buscan obtener acceso. Esto puede sacar del mercado a las empresas basadas en datos existentes o evitar que otras ingresen.*
- **Competencia leal:** *los datos cogenerados no personales crecerán exponencialmente, sin embargo, las reglas que se les asignan se dejan en manos de contratos privados que pueden plantear preguntas relacionadas con la competencia leal.*
- **Secretos comerciales**: *podría requerirse orientación sobre la Directiva sobre secretos comerciales para comprender el papel de apoyo que puede desempeñar cuando las empresas otorgan acceso a sus datos.*
- **Interoperabilidad:** *aborde las "situaciones de bloqueo" en la portabilidad de datos, la interoperabilidad de los contratos inteligentes introduzca un derecho vinculante a la portabilidad B2B, etc.*
- **Régimen de transferencia de datos no personales:** *abordar la protección de la propiedad intelectual y los secretos comerciales para las transferencias de datos no personales a terceros países.*