



Análisis del proceso de transformación digital en las Administraciones Públicas

Analysis of the digital transformation process in Public Administrations

José Joaquín de Haro Navarro

Jefe de Servicio de Modernización Administrativa
y TIC de la Diputación de Albacete

Fecha de recepción: 19/08/2025

Fecha de aceptación: 09/12/2025

Sumario: RESUMEN.—ABSTRACT.—I. INTRODUCCIÓN.—II. EL PANORAMA ACTUAL DEL SECTOR PÚBLICO.—III. LOS IMPRESCINDIBLES DE TODA TRANSFORMACIÓN DIGITAL.—3.1. Esquema Nacional de Seguridad.—3.2. Interoperabilidad.—3.3. Simplificación Administrativa.—3.4. El Factor humano y la Resistencia al cambio.—IV. REUTILIZACIÓN DE SERVICIOS DIGITALES.—4.1. El proyecto Sedipualb@.—V. LA INTELIGENCIA ARTIFICIAL EN LAS ADMINISTRACIONES PÚBLICAS.—5.1. El Reglamento Europeo de IA (AI Act).—5.2. La Soberanía Digital en la era de la Inteligencia Artificial (IA).—VI. LA TRANSFORMACIÓN DIGITAL EN LOS PARLAMENTOS.—VII. CONCLUSIONES.—VIII. BIBLIOGRAFÍA.

RESUMEN

El conjunto de Administraciones Públicas de nuestro país se está sometiendo, en mayor o menor medida, a un proceso de transformación digital que acarrea cambios importantes, tanto en los flujos de información como en las estructuras organizativas. El siguiente estudio trata de abordar una visión del panorama actual, con mención especial hacia los Parlamentos y con una vocación crítica pero constructiva, de mejora continua de los servicios públicos.

PALABRAS CLAVE: *Transformación Digital, sostenibilidad, reutilización, interoperabilidad, inteligencia artificial, simplificación administrativa.*

ABSTRACT

The set of Public Administrations in our country is undergoing, to a greater or lesser extent, a process of digital transformation that entails significant changes, both in information flows and in organizational structures. The following study aims to provide a view

of the current landscape, with a special mention of Parliaments and with a critical yet constructive vocation, for the continuous improvement of public services.

KEYWORDS: Digital Transformation, Sustainability, Reuse, Interoperability, Artificial Intelligence, Administrative Simplification.

I. INTRODUCCIÓN

El conjunto del sector público de nuestro país se encuentra en un proceso de transformación digital sin retorno, que está estableciendo, tanto un nuevo modelo de gestión como de comunicación con la ciudadanía, lo cual afecta de forma directa y no siempre positiva a la eficiencia en la gestión del conjunto de las entidades afectadas.

Adicionalmente, el elefantiásico y heterogéneo modelo del sector público en nuestro país, dificulta la homogeneidad y la coordinación de este proceso de transformación digital que estamos acometiendo en nuestras organizaciones. La comparación con modelos de transformación digital de otros países, como el caso de Estonia, donde ni la población ni la estructura de su administración es para nada equiparable, permite atisbar el amplio espectro de mejora que tenemos en España, algo que debemos ver siempre como una oportunidad de mejora y desde una perspectiva positiva.

Ante esta situación, donde la tecnología avanza a velocidades de vértigo, con la inteligencia artificial presente a todos los niveles de nuestra sociedad y donde la regulación y la organización interna de las Administraciones Públicas están siempre «al rebufo», se plantea un contexto que requeriría un modelo de gobernanza mucho más homogéneo, pero que no tiene visos de producirse y donde el sentido común, la cooperación y la reutilización deben ser nuestros mejores aliados.

II. EL PANORAMA ACTUAL DEL SECTOR PÚBLICO

En España, las Administraciones Públicas se organizan en varios niveles. Según la estructura del Estado y la Ley 40/2015, de Régimen Jurídico del Sector Público, se distinguen cuatro grandes tipos de Administraciones Públicas:

1. Administración General del Estado (AGE):
 - Es el conjunto de órganos centrales del Estado, como ministerios, delegaciones del Gobierno, etc.
2. Administraciones de las comunidades autónomas:
 - Hay 17 comunidades autónomas y 2 ciudades autónomas (Ceuta y Melilla), cada una con su propio gobierno y administración.

3. Administración local:

— Comprende:

- 8.131 municipios (ayuntamientos).
- Diputaciones provinciales (en provincias no uniprovinciales).
- Cabildos insulares (en Canarias) y Consells insulars (en Baleares).
- Comarcas, mancomunidades y otras entidades supramunicipales.

4. Administración institucional o sector público institucional:

- Incluye organismos autónomos, entidades públicas empresariales, agencias, fundaciones públicas, consorcios, etc., tanto del Estado como de comunidades autónomas y entidades locales.

En resumen, tenemos 4 niveles de administración y en torno a 10.000 Administraciones Públicas en España si contamos cada ayuntamiento, diputación, comunidad autónoma, ministerio, etc.

Si se amplía el enfoque para incluir organismos autónomos, entidades públicas empresariales, fundaciones públicas y otros entes del sector público institucional, el número aumenta considerablemente. Según datos de 2021, había un total de 16.851¹ organismos públicos en España, distribuidos de la siguiente manera:

- 317 pertenecientes a la Administración Central
- 1.314 de las comunidades autónomas
- 15.191 de la administración local
- 29 fondos y mutuas dependientes de la Seguridad Social

Este número refleja la complejidad y la descentralización del sector público español, con una amplia variedad de entidades que gestionan competencias y servicios en diferentes niveles. Esta descentralización, siendo positiva para muchos elementos, constituye un gran reto a la hora de homogeneizar la transformación digital de nuestro sector público.

En otro orden de cosas, en 2024 las administraciones públicas en España fueron blanco de un número significativo de ciberataques. Según datos del Centro Criptológico Nacional (CCN-CERT), en los dos primeros meses del año se registraron 25.000 ataques, lo que representó un aumento del 190 % respecto al mismo período del año anterior. Si esta tendencia continuó durante el resto del año, se estima que el total de ciberataques podría haber superado los 150.000².

¹ Libremercado

² El Español

Este incremento se atribuye, en parte, a la actividad de grupos de ciberdelincuentes como LockBit, que intensificaron sus ataques tras la Operación Cronos (*operación policial internacional contra el grupo de ransomware LockBit*). Además, se estima que aproximadamente el 34 % de todos los ciberataques en España en 2024 estuvieron dirigidos al sector público³.

En respuesta a esta creciente amenaza, el Gobierno español aprobó una inversión de 1.157 millones de euros para reforzar la ciberseguridad y la ciberdefensa, con el objetivo de mejorar la prevención, detección y protección frente a amenazas cibernéticas, especialmente en infraestructuras críticas⁴.

En 2024, las administraciones públicas de España realizaron una inversión récord en tecnologías de la información y comunicación (TIC), alcanzando los 8.069 millones de euros, lo que representó un incremento del 34,96 % respecto al año anterior. Entre las empresas que más contratos obtuvieron se encuentran Telefónica, Indra e Inetum, que en conjunto gestionaron 1.753 millones de euros en adjudicaciones, representando el 21,73 % del total invertido por las administraciones durante ese periodo⁵.

Ante este panorama de oportunidad de negocio, además de las grandes empresas existentes en el mercado español, varios fondos de inversión han ido aterrizando a lo largo de los últimos años en nuestro país, adquiriendo determinadas empresas tecnológicas para situarse en condiciones de optar a una parte del «pastel» que supone toda esta pléyade de inversiones que en buena parte provienen de fondos europeos, por ejemplo:

- *AnaCap se hace con la gestión de los impuestos municipales (GTT) por 130 millones de euros*⁶
- *TA Associates compra de la tecnológica española esPublico por más de 500 millones de euros*⁷

Con todo ello, se describe una situación bastante compleja con presencia de diferentes actores, tanto públicos como privados que tiene intereses diferentes pero deben trabajar conjuntamente para poder alcanzar los objetivos marcados.

³ CyberSecurity News

⁴ ElHuffPost

⁵ Channel Partner

⁶ El Confidencial

⁷ Expansión

III. LOS IMPRESCINDIBLES DE TODA TRANSFORMACIÓN DIGITAL

En cualquier transformación digital existen unos elementos imprescindibles que hay que contemplar de forma obligada, vamos a describirlos y comentar sus principales características:

3.1. Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) en España es un marco normativo que tiene como objetivo establecer la política de seguridad en la utilización de medios electrónicos por parte de las administraciones públicas y entidades vinculadas o dependientes de ellas. Constituye un elemento esencial a la hora del cumplimiento de la directiva europea de seguridad NIS2 en el sector público.

A continuación, se presentan los principales elementos del ENS respecto a las entidades públicas:

- Principios Básicos. Son los fundamentos sobre los que se construye la seguridad de la información en el sector público:
 - Seguridad como proceso integral
 - Gestión de riesgos
 - Prevención, detección, respuesta y recuperación
 - Línea de defensa
 - Reevaluación periódica
 - Función diferenciada
 - Responsabilidad
 - Proporcionalidad
 - Seguridad por defecto
 - Seguridad por diseño
 - Eficiencia
- Categorías de los Sistemas. Los sistemas de información se clasifican según el impacto que tendría un incidente de seguridad:
 - Bajo
 - Medio
 - Alto

Esta clasificación afecta la aplicación de las medidas de seguridad exigidas.

- Medidas de Seguridad. Divididas en tres tipos:
 - Organizativas: políticas, procedimientos, control de acceso, etc.
 - Operacionales: gestión de incidencias, continuidad, formación, etc.
 - Técnicas: cifrado, antivirus, firewalls, etc.

Cada medida tiene tres niveles (bajo, medio, alto) en función de la categoría del sistema.

- Organización de la Seguridad. Incluye la definición de roles y responsabilidades dentro de las entidades públicas, como:
 - Responsable de la Información
 - Responsable del Servicio
 - Responsable de Seguridad
 - Responsable del Sistema
- Gestión de Riesgos. Las entidades deben realizar un análisis y gestión de riesgos que sirva de base para aplicar las medidas de seguridad adecuadas. Este proceso debe ser continuo y revisado periódicamente.
- Declaración de Aplicabilidad (DoA). Documento obligatorio que recoge las medidas de seguridad aplicables a un sistema concreto, justifica su aplicación o no aplicación, y su nivel.
- Auditorías de Seguridad. Las entidades deben someter sus sistemas de información a auditorías periódicas (mínimo cada dos años) para garantizar el cumplimiento del ENS.
- Concienciación y Formación. Es obligatorio formar y concienciar al personal sobre sus responsabilidades y buenas prácticas de seguridad.
- Adaptación y Actualización. Con la actualización del ENS en 2022 (Real Decreto 311/2022), se introdujeron nuevas obligaciones, especialmente en ciberseguridad, protección frente a amenazas avanzadas, y requisitos para la seguridad en la nube.
- **Ámbito de Aplicación.** Afecta a:
 - Administraciones públicas (estatal, autonómica, local).
 - Entidades vinculadas o dependientes del sector público.
 - Proveedores del sector privado que presten servicios a entidades públicas (cuando gestionan información o servicios sujetos al ENS⁸).

3.2. Interoperabilidad

La interoperabilidad, en el contexto de los sistemas de información de las administraciones públicas, se refiere a la capacidad de distintos sistemas, servicios o entidades gubernamentales para intercambiar datos y utilizar la información intercambiada de forma efectiva y segura, sin necesidad de intervención

⁸ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

manual. Es un concepto clave e imprescindible para lograr una administración pública más eficiente, transparente y centrada en el ciudadano.

Esta definición está alineada con el Marco Europeo de Interoperabilidad (EIF) y es adoptada en muchas normativas nacionales como la Ley 39/2015 y la Ley 40/2015 en España.

Tipos de interoperabilidad. La interoperabilidad se clasifica en varios niveles, cada uno abordando diferentes aspectos necesarios para garantizar el intercambio eficaz de información:

1. Interoperabilidad Técnica: Se refiere a la compatibilidad de hardware, software, redes y protocolos para permitir el intercambio directo de datos entre sistemas.

Ejemplos:

- Uso de estándares abiertos como XML, JSON, REST, SOAP.
- Conectividad entre plataformas a través de API.

2. Interoperabilidad Semántica. Garantiza que el significado de los datos intercambiados sea entendido de la misma manera por todas las partes.

Ejemplos:

- Uso de vocabularios comunes o catálogos (como el Diccionario de Datos del Sector Público).
- Ontologías compartidas que definen conceptos administrativos como «ciudadano», «resolución», «procedimiento».
- Modelos comunes de información como el definido en el proyecto CODICE de contratación pública.

La interoperabilidad semántica es un elemento clave en los procesos de transformación digital, ya que permite a través de la creación de modelos de información estructurada, la posibilidad de intercambiar conjuntos de datos que responden a un interés común y permiten la automatización de los procesos de gestión asociados.

Casos como el de FACE y facturae o como el ya citado de CODICE y la Plataforma de Contratación del Sector Público, son claros ejemplos de este tipo de interoperabilidad, que es una de las que mayores beneficios genera.

3. Interoperabilidad Organizativa. Asegura que las organizaciones implicadas colaboren eficazmente mediante la alineación de procesos de negocio, responsabilidades y objetivos.

Ejemplos:

- Acuerdos de nivel de servicio (SLA) entre organismos.
- Procesos administrativos alineados para que una solicitud pase por varios entes sin requerir duplicidad.

4. Interoperabilidad Legal. Se refiere a la compatibilidad normativa y jurídica que permite el intercambio y tratamiento legal de la información.

Ejemplos:

- Legislación que habilita el intercambio de datos entre organismos.
- Cumplimiento del RGPD (Reglamento General de Protección de Datos) en la cesión de datos personales.

La interoperabilidad en todas sus facetas, es un elemento imprescindible en la transformación digital de las administraciones públicas, facilitando la tramitación electrónica, reduciendo la carga administrativa a los ciudadanos y empresas. Además mejora la eficiencia y evita duplicidades, favoreciendo a su vez la transparencia y el acceso a la información.

El principio «once only» es una buena práctica que se formalizó y promovió a nivel europeo por la Comisión Europea, especialmente en sus políticas de administración electrónica y digitalización del sector público y se centra en la utilización de la interoperabilidad para no pedir documentos ya presentados.

No obstante, el consumo de información en de los sistemas de interoperabilidad de nuestro país no acaba de despegar, la complejidad de la gestión que hay que realizar para consumir la información disponible, que es amplia y variada, está ralentizando la generalización de esta práctica que es imprescindible, a mi juicio, en todo proceso de transformación digital.

En el marco europeo el Reglamento sobre la Europa Interoperable (Interoperability Act⁹) es una pieza clave en la estrategia de la Unión Europea para digitalizar y modernizar el sector público, facilitando la prestación de servicios públicos digitales transfronterizos de alta calidad.

Su objetivo principal es garantizar un alto nivel de interoperabilidad de los servicios públicos digitales en toda la Unión Europea. Esto implica que las administraciones públicas, tanto a nivel local, regional, nacional como europeo, puedan cooperar y compartir datos y soluciones de manera fluida, eliminando barreras legales, organizativas, semánticas y técnicas.

Se pretende una evaluación de interoperabilidad previa a la toma de decisiones sobre nuevos servicios digitales transeuropeos o modificaciones de los existentes. Los resultados de estas evaluaciones deberán publicarse de forma accesible. Aspectos más destacados:

- Compartición de soluciones y el Portal de la Europa Interoperable: Se establece la obligación de compartir soluciones de interoperabilidad, incluyendo documentación técnica, código fuente y estándares utilizados. Estas soluciones se centralizarán y publicarán en un nuevo

⁹ Interoperable Europe Act | Interoperable Europe Portal

«Portal de la Europa Interoperable», promoviendo la reutilización y el ahorro de costes y tiempo.

- **Habilitación de sandboxes (entornos de prueba):** Se contempla la creación de entornos controlados para probar la interoperabilidad de nuevas soluciones, gestionados bajo supervisión legal, especialmente cuando impliquen datos personales. Esto fomenta la experimentación y la innovación.
- **Gobernanza centralizada:** Se crea un «Comité de la Europa Interoperable» compuesto por representantes de los Estados miembros y de la Comisión Europea. Este comité tendrá como funciones coordinar, supervisar y desarrollar criterios y marcos de interoperabilidad, como el Marco Europeo de Interoperabilidad. Los Estados miembros deberán designar una autoridad competente para la aplicación del Reglamento.
- **Beneficios para ciudadanos y empresas:** La ley busca facilitar la vida de ciudadanos y empresas al mejorar el acceso a servicios públicos digitales transfronterizos (por ejemplo, reconocimiento de títulos, acceso a la seguridad social, intercambio de datos fiscales), lo que se traduce en ahorro de tiempo y dinero, mayor transparencia y una mayor confianza en las administraciones.
- **Reutilización de información pública:** Fomenta la reutilización de información de carácter público de las administraciones, asegurando la persistencia de la información y el uso de formatos y condiciones de uso adecuados.

En resumen, el Reglamento sobre la Europa Interoperable (Interoperability Act) busca construir un ecosistema de administraciones públicas digitales interconectadas en la UE, facilitando la colaboración transfronteriza y acelerando la transformación digital del sector público para beneficio de todos.

3.3. Simplificación Administrativa

La simplificación es un objetivo intrínseco a los esfuerzos de modernización y digitalización de las administraciones públicas. Su propósito principal es reducir las barreras burocráticas y mejorar la prestación general de los servicios.

Es crucial comprender que la transformación digital va más allá de la mera digitalización de documentos en papel, demandando una revisión fundamental de los procesos existentes, una reducción significativa de las cargas administrativas y el aprovechamiento estratégico de las plataformas de intermediación de datos. Se trata de optimizar el funcionamiento administrativo en su conjunto,

adaptándose rápidamente a los cambios del entorno y promoviendo un uso inteligente y eficiente de los recursos disponibles.

Se hace imprescindible una reingeniería de procesos¹⁰ y una simplificación documental, la simplificación no es un beneficio colateral ni un paso posterior, sino un requisito fundamental y un principio rector para una transformación digital eficaz. Por lo tanto, un replanteamiento radical y un rediseño de la forma en que se prestan los servicios públicos deben preceder o ejecutarse en paralelo con la implementación tecnológica para asegurar que la tecnología sirva para simplificar y optimizar, en lugar de simplemente replicar o agravar las complejidades existentes.

Tipos de Reingeniería:

- Reingeniería Administrativa: Se centra en transformar las prácticas de gestión de una organización. Aborda específicamente áreas como los procesos de toma de decisiones, la asignación de recursos y los flujos de comunicación interna para optimizar el funcionamiento administrativo. Su meta es permitir que las organizaciones operen de manera más eficiente y alineadas con sus objetivos estratégicos, promoviendo una utilización inteligente de los recursos. Este enfoque a menudo implica la implementación de nuevas herramientas tecnológicas, metodologías ágiles y estructuras de trabajo dinámicas.
- Reingeniería Organizacional: Implica un rediseño integral tanto de la estructura como de la cultura subyacente de la empresa. El objetivo es modernizar las operaciones y mejorar el rendimiento global. Esto puede incluir la redefinición de roles y responsabilidades, la simplificación de las jerarquías y el fomento de relaciones más colaborativas entre el personal. Más allá de los cambios estructurales, enfatiza el cultivo de una cultura organizacional innovadora y flexible, lo que ayuda a eliminar barreras burocráticas y fomenta la participación activa de los equipos, conduciendo a una mayor creatividad, una mejor comunicación y una toma de decisiones más ágil.

La simplificación de procesos administrativos, impulsada por la transformación digital, genera un amplio espectro de beneficios que impactan directamente en la calidad de vida de los ciudadanos y en la competitividad de las empresas, fomentando una relación más eficiente y transparente con la administración pública, podemos destacar los siguientes:

- Mejora de la Eficiencia y Reducción de Costes: La digitalización del sector público conduce a una mejora sustancial de la eficiencia y a una significativa reducción de costes. La automatización de procesos, previa simplificación, libera a los funcionarios de tareas repetitivas,

¹⁰ Instituto de Innovación Digital de las Profesiones (INESDI).

permitiéndoles enfocarse en actividades de mayor valor. Esto no solo optimiza el uso de los recursos públicos, sino que también alivia las presiones de austeridad fiscal que enfrentan los gobiernos.

- Mayor Transparencia y Rendición de Cuentas: Una transformación digital asentada en procesos consolidados y previamente revisados facilita una mayor transparencia en las actuaciones, permitiendo a ciudadanos y organizaciones acceder a información relevante de manera rápida y sencilla a través de plataformas digitales y portales de datos abiertos. Esta transparencia es fundamental para fomentar la confianza en las instituciones públicas, ya que la capacidad de rastrear y verificar el uso de los recursos y las decisiones administrativas refuerza la rendición de cuentas y ayuda a prevenir la corrupción.

3.4. El Factor humano y la Resistencia al cambio

La transformación digital en la administración pública no es solo una cuestión de tecnología, sino fundamentalmente de personas. El enfoque debería trasladarse a cómo esta transformación mejora la vida de los ciudadanos y de los propios empleados públicos, pero en el caso de estos últimos la gestión del factor humano es uno de los grandes retos de todo proceso de transformación digital.

Podemos identificar los siguientes aspectos importantes a la hora de afrontar la gestión del Factor humano:

- Gestión del Talento y Nuevos Perfiles Profesionales:
 - Obsolescencia profesional: Muchos empleados públicos pueden sentir que sus habilidades actuales no se ajustan a las nuevas demandas digitales. Es fundamental pasar de una gestión de personal tradicional a una gestión del talento, que fomente el desarrollo de nuevas competencias.
 - Competencias digitales: Es indispensable que los empleados públicos, independientemente de su puesto, adquieran competencias digitales básicas y avanzadas. Esto incluye no solo el manejo de herramientas, sino también la capacidad de trabajar con datos, comprender algoritmos y adaptarse a nuevos procesos.
 - Perfiles especializados: La administración pública necesita profesionales capaces de dinamizar la transformación digital, con perfiles específicos en posiciones estratégicas y transversales (ej. analistas de datos, expertos en ciberseguridad, gestores de proyectos digitales, etc.).
 - Intra-emprendedores públicos: Impulsar el liderazgo de aquellos empleados con vocación de servicio e iniciativa para pro-

mover la innovación interna, ya que en muchos casos son los verdaderos generadores de la innovación y la mejora de los servicios públicos.

— Cultura Organizacional y Liderazgo:

- Cambio de paradigma: La transformación digital implica un profundo cambio de mentalidad, pasando de un enfoque burocrático basado en procedimientos a uno centrado en la toma de decisiones basada en datos y la innovación.
- Liderazgo transformador: Es crucial contar con líderes en todos los niveles que articulen una visión clara del futuro digital, fijen objetivos ambiciosos, cuestionen el statu quo y promuevan el cambio. Los directivos deben ser los primeros en poseer competencias digitales y estar dispuestos a liderar con el ejemplo.
- Cultura de innovación y adaptabilidad: Fomentar un entorno que valore la experimentación, el aprendizaje continuo y la adaptabilidad.
- Comunicación, Participación y Formación: Escucha activa: Proporcionar a los empleados públicos herramientas y espacios para expresar propuestas y mejoras.
- Comunicación clara: Explicar los motivos y beneficios de los cambios para generar comprensión y aceptación.
- Formación continua: Invertir en programas de capacitación exhaustivos y globales que permitan a los empleados adquirir las habilidades necesarias para los nuevos entornos digitales.
- Implicación: Incluir a los empleados en el proceso de cambio, permitiéndoles participar y contribuir en el diseño e implementación de las nuevas soluciones. Esto genera sentido de pertenencia y compromiso.

La resistencia al cambio es uno de los mayores obstáculos internos en la transformación digital del sector público, es el principal causante de la parálisis que se atribuye a cualquier proceso de reforma que se inicia en nuestras administraciones y merece un apartado especial para poder comprender sus causas y poder abordarla eficazmente:

- Familiaridad y comodidad: Las personas tienden a sentirse seguras en entornos conocidos. La introducción de cambios puede generar incertidumbre y amenaza a esta sensación de seguridad.
- Miedo a lo desconocido: La ansiedad sobre cómo los cambios afectarán las rutinas, roles y resultados puede paralizar a los empleados. «Más vale malo conocido que bueno por conocer» es una frase que a menudo resume esta mentalidad.

- Pérdida de poder o control: Los cambios suelen implicar una redistribución de roles y responsabilidades. Aquellos que perciben una pérdida de estatus o control pueden resistirse activamente.
- Falta de comprensión o información: La ausencia de una comunicación clara y transparente sobre el propósito, beneficios y cómo se llevarán a cabo los cambios puede generar desconfianza y resistencia.
- Cultura organizacional: Muchas administraciones públicas tienen culturas organizacionales arraigadas, a menudo burocráticas que no fomentan la innovación y la adaptabilidad.
- Sistemas heredados y obsolescencia tecnológica: La dependencia de sistemas obsoletos puede dificultar la integración con nuevas tecnologías, frustrando a los empleados y reforzando la percepción de que «siempre se ha hecho así».
- Brecha de competencias: La falta de habilidades digitales entre los empleados puede generar inseguridad y miedo a no poder adaptarse a las nuevas herramientas y procesos.

Para mitigar la resistencia al cambio y asegurar el éxito de la transformación digital, es crucial implementar estrategias de gestión del cambio efectivas:

- Liderazgo y visión clara: Los líderes deben comunicar una visión convincente del futuro digital, resaltando los beneficios para la organización, los empleados y los ciudadanos.
- Comunicación transparente y constante: Mantener informados a los empleados sobre el progreso, los desafíos y los éxitos. Crear canales de feedback donde puedan expresar sus inquietudes.
- Participación y co-creación: Involucrar a los empleados en el diseño y la implementación de las soluciones digitales. Cuando se sienten parte del proceso, la aceptación es mayor.
- Capacitación y desarrollo de habilidades: Proporcionar programas de formación continuos y personalizados que aborden las nuevas competencias digitales requeridas. El apoyo continuo durante la transición es clave.
- Reconocimiento y celebración de logros: Destacar y recompensar los esfuerzos y éxitos en la adopción de nuevas prácticas y tecnologías.
- Gestión de expectativas: Ser realistas sobre los desafíos y el tiempo que llevará la transformación.
- Fomentar una cultura de experimentación y aprendizaje: Permitir el «error controlado» y aprender de él para ajustar las estrategias.

La transformación digital en el sector público es un desafío que requiere un enfoque holístico, donde la tecnología es un medio y no un fin. El éxito dependerá en gran medida de cómo se gestione el capital humano, superando la resistencia al cambio a través de un liderazgo fuerte, una comunicación efectiva, una formación adecuada y una cultura que promueva la innovación y la adaptabilidad.

IV. REUTILIZACIÓN DE SERVICIOS DIGITALES

Aunque no existe una «Directiva de Reutilización de Software» específica como tal, la promoción de la reutilización de software se integra en marcos más amplios:

1. Reglamento sobre la Europa Interoperable (Interoperability Act):

Este reglamento es, con diferencia, la pieza legislativa más relevante en este ámbito. Uno de sus objetivos principales es facilitar y promover la reutilización de soluciones de software y componentes tecnológicos entre las administraciones públicas de la UE.

Busca establecer un marco común que impulse la interoperabilidad transfronteriza y la colaboración en el desarrollo de soluciones digitales. Esto incluye la creación de catálogos y plataformas centralizadas para compartir y descubrir software desarrollado por las AP.

Es probable que este Reglamento establezca la obligatoriedad o, al menos, un fuerte incentivo para que las administraciones consideren el software de código abierto y la reutilización como opciones por defecto en sus adquisiciones y desarrollos.

2. Marco Europeo de Interoperabilidad (European Interoperability Framework – EIF):

El EIF, aunque no es un texto legal vinculante en sí mismo, es un conjunto de recomendaciones y principios que guían a las administraciones públicas europeas en la prestación de servicios digitales interoperables.

La reutilización es uno de los principios fundamentales del EIF. Destaca la importancia de reutilizar conceptos, aplicaciones, servicios, especificaciones, modelos de datos y fuentes de información administrativa.

Promueve activamente el uso de software de código abierto como facilitador clave de la reutilización y la interoperabilidad, ya que reduce la dependencia de proveedores privados, fomenta la transparencia y permite la colaboración en el desarrollo.

3. Estrategia Europea de Datos y Estrategia Digital de la UE:

Aunque se centran más en los datos, estas estrategias reconocen que una infraestructura digital sólida y la capacidad de las administraciones para desarrollar y compartir soluciones de software son esenciales para construir una «Europa Digital». La reutilización de software contribuye directamente a estos objetivos al reducir costes, acelerar el desarrollo y fomentar la colaboración.

4. Iniciativas y Herramientas Concretas:

Más allá de la legislación general, la Comisión Europea ha impulsado varias iniciativas concretas para fomentar la reutilización de software:

— Portal «Interoperable Europe» (anteriormente ISA² Programme):

Este portal es un centro neurálgico para la interoperabilidad en Europa. Dentro de él, existe una sección dedicada específicamente a la «Sharing and Reuse of IT Solutions» (Compartición y Reutilización de Soluciones TI).

Aquí podemos encontrar:

- «The Sharing and Reuse Framework for IT Solutions»: Un marco que proporciona recomendaciones sobre cómo las administraciones públicas pueden compartir, reutilizar o desarrollar soluciones TI.
- «Sharing & Reuse Awards»: Concursos para reconocer y promover las mejores prácticas en la reutilización de soluciones TI en las administraciones públicas europeas.
- Comunidades y recursos: Espacios para que las administraciones compartan experiencias, publiquen soluciones y encuentren herramientas para la reutilización.

— Joinup Platform:

Es una plataforma colaborativa y un catálogo de soluciones digitales interoperables para las administraciones públicas. Permite a las entidades públicas de toda Europa compartir y reutilizar software, especificaciones, directrices y otros activos digitales. Es un lugar clave donde las administraciones pueden publicar su software de código abierto para que otros lo reutilicen y lo mejoren.

— Política de Código Abierto de la Comisión Europea (Open Source Software Strategy):

La Comisión Europea ha adoptado su propia estrategia de software de código abierto, reconociendo los beneficios del OSS para la apertura, la transparencia, la seguridad y la reutilización.

Esta política busca que la propia Comisión libere su software bajo licencias de código abierto siempre que sea posible, dando ejemplo a los Estados miembros.

- Licencia Pública de la Unión Europea (EUPL – European Union Public Licence):

Es una licencia de software libre y de código abierto específicamente diseñada para su uso por las administraciones públicas europeas. Permite que el software desarrollado con fondos públicos se distribuya y reutilice fácilmente por otras administraciones y el público en general, garantizando la compatibilidad legal transfronteriza. La EUPL es un instrumento clave para facilitar la reutilización de software en el contexto europeo.

- Estudios e Informes sobre el Impacto del Software Libre:

La UE ha encargado y publicado estudios que demuestran el ahorro significativo que la reutilización de software libre genera para las administraciones públicas, así como los beneficios en términos de soberanía tecnológica, innovación y colaboración.

Retos y Enfoques:

A pesar de estas iniciativas, la reutilización de software entre administraciones públicas sigue enfrentando desafíos, como:

- Diferencias normativas y técnicas: Aunque la EUPL ayuda, las leyes de contratación pública, los requisitos de seguridad y los marcos tecnológicos pueden variar.
- Falta de conocimiento: Muchas administraciones pueden no ser conscientes del software ya existente o de los beneficios de la reutilización.
- Cultura de «no inventar la rueda»: A veces, puede parecer más fácil encargar un nuevo desarrollo que adaptar y reutilizar una solución existente.
- Mantenimiento y soporte: La sostenibilidad del software reutilizado requiere modelos claros de mantenimiento y soporte, a menudo basados en comunidades.

Para abordar estos retos, el enfoque europeo se centra en:

- Fomentar el software de código abierto: Al ser el código abierto accesible y modificable, es inherentemente más propicio para la reutilización.

- Crear catálogos y plataformas centralizadas: Facilitar la búsqueda y el descubrimiento de software reutilizable.
- Proporcionar directrices y marcos (como el EIF y el Sharing and Reuse Framework): Orientar a las administraciones sobre las mejores prácticas.
- Incentivar la colaboración: Promover el codesarrollo de soluciones entre diferentes administraciones.

En definitiva, la reutilización de software por parte de las administraciones públicas en Europa es una prioridad estratégica, impulsada por un marco de interoperabilidad creciente, el fomento del código abierto y la creación de herramientas y plataformas colaborativas para maximizar la eficiencia y la innovación en el sector público digital.

4.1. El proyecto Sedipualb@¹¹

En España la reutilización de servicios digitales se ha abordado desde el punto de vista jurídico en la ley 40/2015 de Régimen Jurídico del Sector Público, concretamente en su artículo 157, donde se establece lo siguiente:

«Artículo 157. Reutilización de sistemas y aplicaciones de propiedad de la Administración.

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomenta con ello la incorporación de los ciudadanos a la Sociedad de la información.

3. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total

¹¹ www.sedipualba.es

o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera».

Es muy importante resaltar que se impone la obligación a las AAPP de acudir al directorio general de aplicaciones de la Administración General del Estado, antes de realizar una licitación pública para adquirir una solución de este tipo en el mercado.

En nuestro país tenemos un ejemplo de reutilización de servicios digitales que aglutina gran parte de los elementos necesarios para definirse como una buena práctica en este sentido, de hecho fue premiado en 2027 por la Comisión Europea en los «Share and Reuse Awards» celebrados en Lisboa.

El proyecto Sedipualb@, creado y desarrollado por la Diputación de Albacete, es un ejemplo de reutilización de herramientas de software, que se ha convertido en un referente en el ámbito de la gestión administrativa de entidades del sector público.

Características esenciales del proyecto:

- Desarrollo propio con emplead@s públicos: Un elemento esencial que facilita la reutilización de los servicios digitales es que el desarrollo de los mismos se realice con medios propios por parte de la administración, ya que de esta forma se dispone de todos los elementos necesarios para una evolución continua del servicio, sin dependencias externas.

La reutilización en proyectos digitales donde existe una participación externa, a través de una licitación pública, tiene varias dificultades derivadas de la posibilidad de que esta reutilización genere ventajas competitivas en el mercado.

- Escalabilidad: Se refiere a la capacidad de un sistema, aplicación o proceso para manejar una cantidad creciente de trabajo o usuarios sin comprometer su rendimiento, eficiencia o funcionalidad. Esencialmente, se trata de la habilidad del software para crecer y expandirse de manera efectiva a medida que aumentan las demandas.

Sedipualb@ está diseñado desde su inicio con esta premisa, ya que se trata de un elemento imprescindible y determinante en la posterior evolución de este tipo de proyectos.

- Sostenibilidad: Se refiere a la capacidad de un proyecto para generar y mantener los recursos financieros necesarios para operar, perdurar y seguir siendo viable a lo largo del tiempo, una vez finalizada la financiación inicial o externa. No se trata solo de la rentabilidad a corto plazo, sino de la habilidad para ser autosuficiente y generar valor económico de manera continua, sin comprometer los recursos futuros ni generar dependencias insostenibles.

El proyecto Sedipualb@ dispone de modelo de financiación que se articula para permitir imputar y sufragar todos los costes involucrados en el mismo, desde una perspectiva *sin ánimo de lucro*.

- Liderazgo e Intraemprendimiento: El liderazgo se refiere como la capacidad de influir y guiar a un equipo de personas hacia el logro de los objetivos del proyecto, a través de la visión, la motivación, la dirección y la facilitación de un ambiente de trabajo colaborativo y productivo.

El proyecto Sedipualb@ ha sido creado por personas pertenecientes a la Diputación de Albacete, desde una perspectiva multidisciplinar, contando con profesionales de diferentes ámbitos (económico, jurídico y TIC) y es liderado por el Servicio de Modernización Administrativa y TIC (SEMATIC) de la propia Diputación de Albacete.

Este intraemprendimiento es sin duda un elemento habilitador y motivador dentro de la organización, de cara a estimular a la misma a moverse en la dirección adecuada para la correcta continuidad del proyecto.

- Colaboración administrativa: Uno de los elementos más representativos de este proyecto es su capacidad generadora de colaboración administrativa real, de forma que se produce una interacción entre dos o más administraciones pública en torno a resolver una determinada problemática común, siempre con el objetivo de mejorar los servicios prestados a la ciudadanía.

El proyecto Sedipualb@ establece un marco de colaboración inmejorable, poniendo en común a los diversos agentes involucrados en los procesos de transformación digital de las diferentes administraciones públicas, para que puedan complementar y enriquecer sus procedimientos de gestión.

- Cautividad tecnológica: La cautividad tecnológica es una situación en la que un usuario, una organización o incluso una sociedad, se vuelve dependiente de una tecnología, producto o proveedor particular, de tal manera que resulta extremadamente difícil y costoso cambiar a una alternativa, incluso si esta alternativa fuera superior, más eficiente o más económica a largo plazo.

Esta dependencia se crea debido a una combinación de factores que aumentan los «costes de cambio». Estos costes no son solo monetarios, sino que pueden incluir:

- **Inversión inicial:** Grandes inversiones en infraestructura, software o hardware específicos de un proveedor.
- **Formación y conocimiento:** El personal se ha capacitado en el uso de una tecnología específica, y re-capacitarlo para otra sería costoso y llevaría tiempo.
- **Integración de sistemas:** Los sistemas existentes están fuertemente interconectados con la tecnología cautiva, y desvincularlos requeriría una reingeniería compleja y costosa.
- **Migración de datos:** El traslado de grandes volúmenes de datos de un formato o plataforma a otra puede ser técnicamente complejo, propenso a errores y muy caro.
- **Estándares propietarios:** El uso de formatos de archivo, protocolos o interfaces que son propiedad de un proveedor y no son interoperables con otras soluciones.
- **Contratos a largo plazo:** Acuerdos contractuales que penalizan la salida o el cambio.
- **Efectos de red:** Cuando el valor de una tecnología aumenta a medida que más personas la usan (por ejemplo, redes sociales, sistemas operativos dominantes), lo que desincentiva el cambio a alternativas con menos usuarios.

En el contexto de la administración pública, la cautividad tecnológica presenta riesgos significativos:

- **Pérdida de flexibilidad y agilidad:** Dificulta la adopción de nuevas tecnologías que podrían ofrecer mejores servicios o mayor eficiencia.
- **Dependencia estratégica:** La administración queda a merced de las condiciones, precios y evolución tecnológica de un único proveedor, lo que puede limitar su capacidad de negociación.
- **Costes elevados a largo plazo:** Aunque la inversión inicial en una tecnología propietaria pueda parecer atractiva, los costes de mantenimiento, licencias y futuras actualizaciones pueden ser muy altos debido a la falta de competencia.
- **Dificultad para innovar:** La cautividad puede frenar la innovación al desincentivar la búsqueda y experimentación con soluciones más modernas o adaptadas a las necesidades cambiantes.
- **Riesgos de seguridad:** La dependencia de una única solución o proveedor puede concentrar los riesgos de seguridad y hacer a la administración más vulnerable a fallos o ataques.

La cautividad tecnológica sólo puede evitarse utilizando, soluciones abiertas y reutilizables que promuevan el trabajo colaborativo y no estén exclusivamente en manos de empresas tecnológicas.

Una de los principales objetivos del proyecto Sedipualb@, es luchar contra la cautividad tecnológica existente en los mercados de herramientas de esta naturaleza, donde se está produciendo una gran concentración en manos de unas pocas grandes empresas, lo que está ya generando muchas de las situaciones o riesgos que se han comentado anteriormente.

El proyecto Sedipualb@ es un caso singular de éxito en un contexto de generación de soluciones tecnológicas, habitualmente reservado a empresas de un tamaño medio-alto y con grandes concentraciones de recursos financieros.

Su continuidad a lo largo ya de más de 10 años en un mercado tan exigente como el tecnológico, así como su capacidad de adaptación a los cambios lo han convertido en una alternativa real y efectiva dentro del mercado «Govtech» que cuenta cada día con más administraciones públicas como usuarias.

V. LA INTELIGENCIA ARTIFICIAL EN LAS ADMINISTRACIONES PÚBLICAS

La inteligencia artificial (IA) es una disciplina de las ciencias de la computación que busca crear sistemas y algoritmos capaces de realizar tareas que normalmente requieren inteligencia humana. En esencia, la IA utiliza datos, modelos matemáticos y capacidad computacional para resolver problemas, aprender de la experiencia y tomar decisiones.

La IA no se limita a una sola tecnología, sino que abarca un conjunto de ellas como el aprendizaje automático (machine learning), el aprendizaje profundo (deep learning) y el procesamiento del lenguaje natural (NLP).

Ejemplos de utilización de IA en el las AAPP:

— Servicios al ciudadano y gestión administrativa:

- Asistentes virtuales y chatbots: Permiten a los ciudadanos obtener respuestas a preguntas frecuentes, realizar trámites y recibir información sobre servicios públicos las 24 horas del día.
- Automatización de procesos: La IA puede automatizar tareas repetitivas y que consumen mucho tiempo, como el procesamiento de solicitudes de subvenciones o la revisión de documentos, liberando a los funcionarios para que se centren en labores más complejas.
- Análisis de datos para políticas públicas: La IA puede analizar grandes volúmenes de datos demográficos y sociales para ayudar

a los gobiernos a diseñar políticas más efectivas y a tomar decisiones estratégicas basadas en evidencia.

— Seguridad y prevención:

- Seguridad pública: La IA ayuda a las fuerzas del orden a analizar grandes cantidades de datos para predecir y prevenir la delincuencia, identificar patrones y asignar recursos de manera más eficiente.
- Ciberseguridad: Los sistemas de IA pueden monitorear las redes de forma autónoma para detectar y responder a ciberataques y amenazas en tiempo real.
- Prevención de fraudes: La IA detecta patrones anómalos en transacciones financieras o solicitudes de beneficios, ayudando a identificar fraudes y pagos indebidos.

— Sanidad y bienestar social:

- Gestión de la salud pública: La IA puede analizar datos médicos para predecir brotes de enfermedades, optimizar la distribución de recursos sanitarios y personalizar tratamientos.
- Servicios sociales: Se utilizan algoritmos de IA para identificar a poblaciones en riesgo y garantizar que reciban la ayuda necesaria, como en la protección de la infancia.

— Infraestructuras y movilidad:

- Ciudades inteligentes: La IA contribuye a la gestión del tráfico y la movilidad urbana, prediciendo congestiones y optimizando rutas. También se utiliza para monitorizar la calidad del aire y gestionar los residuos de manera más eficiente.
- Mantenimiento predictivo: La IA puede predecir fallos en infraestructuras críticas (carreteras, puentes, redes eléctricas) para realizar mantenimientos preventivos y reducir costos.

Se trata sin duda de una gran oportunidad de generar eficiencia en la gestión de los servicios públicos, que debemos ser capaces de aprovechar en nuestras Administraciones Públicas siendo conscientes también de los riesgos que la acompañan.

El debate está sobre la mesa ¿cómo afectará la utilización de la IA en nuestras vidas y en nuestros trabajos?, ¿cómo abordar esta disrupción a todos los niveles desde una perspectiva ética, pero que no limite los avances y mejoras que puede generarnos?, son muchas las dudas existentes pero no cabe duda que se irán dilucidando en los próximos años.

5.1. El Reglamento Europeo de IA (AI Act)

En este sentido en Europa se ha dado un primer paso importante en cuanto a la regulación del uso de la IA, a través del Reglamento de Inteligencia Artificial¹², que establece un marco legal para regular la IA en la Unión Europea, con el objetivo de garantizar la seguridad, la protección de los derechos fundamentales y la libre circulación de los sistemas de IA. Este reglamento se aplica a sistemas de IA que se comercialicen, pongan en servicio o se utilicen en la UE, independientemente de si el proveedor tiene su sede dentro o fuera del bloque UE.

Elementos Clave del Reglamento:

El Reglamento adopta un enfoque basado en el riesgo, clasificando los sistemas de IA en cuatro categorías principales según el daño potencial que puedan causar.

— Riesgo Inadmisibile:

Estos sistemas son considerados una clara amenaza para la seguridad, los derechos y las libertades de las personas. Su uso está completamente prohibido. Ejemplos incluyen:

- Sistemas de puntuación social por parte de gobiernos o empresas.
- Uso de técnicas subliminales o manipuladoras que puedan causar daños significativos.
- Reconocimiento de emociones en entornos laborales y educativos.
- Identificación biométrica en tiempo real en espacios públicos (con excepciones muy limitadas para la aplicación de la ley).

— Alto Riesgo:

Los sistemas de alto riesgo son aquellos que pueden tener un impacto significativo en la salud, la seguridad o los derechos fundamentales de las personas. Antes de ser comercializados, deben someterse a requisitos estrictos y a una evaluación de conformidad. Algunos ejemplos de sistemas de alto riesgo son los utilizados en:

- Infraestructuras críticas (gestión del agua, gas, electricidad, etc.)
- Educación (acceso, evaluación o selección de estudiantes)
- Recursos humanos (contratación o selección de personal)
- Sistemas de seguridad y aplicación de la ley.

¹² Reglamento Inteligencia Artificial UE.

— Riesgo Limitado:

En esta categoría se incluyen sistemas que, aunque no se consideran de alto riesgo, requieren que los usuarios sean conscientes de que están interactuando con una IA. Esto es para garantizar la transparencia y la confianza. Ejemplos son:

- Chatbots y asistentes de voz que deben indicar claramente que son sistemas automatizados.
- Contenidos generados o manipulados artificialmente, como las imágenes deepfake, que deben ser etiquetados como tales.

— Riesgo Mínimo o Nulo:

La gran mayoría de los sistemas de IA, como los filtros de spam, los videojuegos o las herramientas de traducción, se consideran de riesgo mínimo. Estos sistemas no están sujetos a obligaciones específicas, aunque se anima a las empresas a adoptar códigos de conducta voluntarios.

Plazos de Puesta en Marcha:

El reglamento entró en vigor en agosto de 2024, pero su aplicación es gradual, con diferentes plazos para cada tipo de sistema:

- Desde agosto de 2024: Entrada en vigor del reglamento.
- Desde febrero de 2025: Se aplican las prohibiciones sobre los sistemas de riesgo inadmisibles. Comienzan los requisitos de alfabetización en IA, exigiendo a los proveedores y usuarios de IA que garanticen que su personal comprende el funcionamiento y los riesgos de estos sistemas.
- Desde agosto de 2025: Se establecen las normas sobre sanciones y multas para los Estados miembros. Los Estados miembros deben informar a la Comisión sobre los recursos de sus autoridades competentes.
- Desde agosto de 2026: Entran en vigor la mayoría de las normas, incluyendo las obligaciones para los sistemas de alto riesgo.
- Los Estados miembros deben establecer al menos un sandbox regulatorio para la IA, un entorno controlado para probar estos sistemas.
- Desde agosto de 2027: Aplicación de los requisitos para los sistemas de IA de alto riesgo que ya existían antes de la entrada en vigor del reglamento.

El RIA actúa únicamente en la regulación del mercado derivado de las actuaciones que utilicen IA, no va mucho más allá de esa clasificación de grupos de riesgo, lo cual ha sido criticado por determinados sectores más proteccionistas de la sociedad, de la misma forma que las ampliaciones regulatorias realizadas por otras administraciones, como la realizada por el gobierno de Asturias (Decreto 98/2025), han sido criticadas por los sectores más liberales.

Se trata sin duda de un terreno complejo y con muchas aristas, en el que es fácil hablar a posteriori, pero muy difícil adivinar el tipo de posicionamiento por parte de las AAPP que será más beneficioso de cara al futuro.

5.2. La Soberanía Digital en la era de la Inteligencia Artificial (IA)

La IA está cambiando la manera de recopilar, procesar y analizar los datos, creando un nuevo marco donde se establece una gran relevancia tanto a la soberanía de los datos, entendida como *la idea de que una entidad tiene la autoridad y el derecho de gobernar y controlar los datos generados dentro de su contexto*, como a la soberanía de las infraestructuras digitales que utiliza.

La excesiva dependencia tecnológica de nuestras Administraciones Públicas, debido a que muchas de las herramientas de IA más potentes son desarrolladas por grandes empresas tecnológicas extranjeras, podría generar una pérdida del control sobre sus datos y procesos. Esto no solo genera una dependencia tecnológica, sino que también expone al Estado a posibles injerencias de gobiernos o empresas extranjeras.

Este problema de dependencia tecnológica no es nuevo en nuestro sector público, ya que desde hace años la mayoría de Administraciones Públicas han optado por soluciones tecnológicas privadas para cubrir el amplio y variado abanico de necesidades que se tienen en este sector.

En una Administración del siglo XXI, que es totalmente digital, quizás merezca la pena realizar una reflexión sobre cómo debemos consumir y de qué forma deben generarse las herramientas tecnológicas que van a coordinar nuestras acciones y generar un gran espacio de datos que sino está bajo nuestro control puede convertirse en un gran problema.

VI. LA TRANSFORMACIÓN DIGITAL EN LOS PARLAMENTOS

La transformación digital en los parlamentos autonómicos sigue avanzando, pero de forma desigual, problemas comunes y ya descritos en este estudio como la interoperabilidad con administraciones, normativa procesal y reglamentaria de las cámaras (adaptación a tramitación electrónica), ciberseguridad, brecha digital interna (funcionarios/representantes), son elementos

que están presentes en estas organizaciones, de la misma forma que el resto de nuestro sector público.

Los sistemas de gestión parlamentaria se han ido adaptando a la gestión digital, junto con la presencia de las Sedes Electrónicas de los distintos parlamentos y una de las claves son los sistemas de integración entre estos entornos, junto con el resto de aplicativos tecnológicos de que disponga cada entidad.

Al no existir una conexión directa con la ciudadanía, como puede ocurrir en otras entidades del sector público, como Ayuntamientos, los avances en transformación digital han sido más dispares y se ha producido una asimetría entre los distintos parlamentos que poco a poco se está corrigiendo.

Las aproximaciones utilizadas por los diferentes parlamentos son variadas y a este respecto sería deseable una mayor coordinación entre ellos, partiendo si cabe de que existen varios movimientos asociativos tanto en el subsistema de tecnologías de información de los parlamentos de nuestro país (ParlaTIC) como en otros colectivos también implicados en la transformación digital, como *letrad@s* y *archiver@s*. Este tejido asociativo de profesionales que trabajan en los parlamentos de nuestro país, es sin duda un perfecto caldo de cultivo para esa coordinación tan necesaria en una materia estratégica como es la transformación digital de estas entidades.

Existe una corriente ya secundada por varios parlamentos (Cortes de Castilla la Mancha, Asamblea Regional de Murcia, Parlamento de las Islas Baleares, Parlamento de La Rioja y Asamblea de Madrid) que utilizan tecnología pública y reutilizable, como es la plataforma *Sedipualb@*, ya citada en este estudio, realizando un ejercicio de colaboración entre entidades que está dando lugar a sinergias realmente interesantes.

VII. CONCLUSIONES

El sector público en nuestro país se encuentra inmerso en un proceso sin retorno de transformación digital, que involucra grandes cambios organizativos y estructurales dentro de las propias entidades. Adicionalmente la heterogeneidad normativa, el gran número de entidades afectadas y la estructura competencial de nuestro país hace todavía más difícil que ese proceso se lleve a cabo con una mayor armonía. Estas dificultades no pueden ser una excusa para que intentemos realizar este tránsito con rigor y tomando las mejores decisiones posibles y apostando por procesos y tecnologías contrastadas.

La coordinación entre las Administraciones Públicas en materias estratégicas como la ciberseguridad (CCN-CERT¹³), interoperabilidad, plataformas comunes como (DIR3, DeHú, SIR, REPRESENT@, CI@VE, @FIRMA, Carpeta Ciudadana, PLACSP, etc.) coordinadas tanto por la AEAD¹⁴ como

¹³ Centro Criptológico Nacional.

¹⁴ Agencia Estatal de Administración Digital.

por los diversos organismos autonómicos con competencias similares (Ej. AOC¹⁵) es sin duda uno de los elementos imprescindibles, pero no suficiente para esta transformación.

Para afrontar este reto con garantías las Administraciones Públicas de todos los niveles (Ayuntamientos, Mancomunidades, Diputaciones, Cabildos, Consells, Comunidades Autónomas, etc.) deben afrontar, dentro de su marco competencial, unas estrategias consensuadas y donde se abandonen los egos territoriales y prevalezca el sentido común, la colaboración interadministrativa y la reutilización de servicios digitales como principios básicos de este proceso.

Merece también especial reflexión, la situación de soberanía de la información y cautividad tecnológica que se puede generar sino tenemos un mayor protagonismo en la creación de nuestros propios servicios digitales y confiamos estas tareas de forma absoluta al sector privado, sobre todo con la llegada de la Inteligencia Artificial, que nos introduce en un nuevo contexto donde la soberanía de los datos sobre los que actúa va a convertirse en un tema estratégico.

La situación de España en los rankings mundiales de transformación digital del sector público es bastante buena en general, pero no debemos dejarnos llevar por estas listas precocinadas, sino continuar robusteciendo nuestro marco de servicios digitales a través de los elementos que se han destacado humildemente en este estudio y los que se propongan dentro de un marco de consenso técnico y procedimental.

La tecnología no es un fin en sí mismo, pero en un mundo digital como el que vivimos, la configuración de las herramientas que use una organización en materias como dependencia tecnológica, sostenibilidad, capacidad de integración con otros sistemas y acceso a los datos generados; es clave y determinante en la capacidad de gestión de la misma.

VIII. BIBLIOGRAFÍA

- Arroyo Yanes, L. M. (2018). La digitalización de las administraciones públicas y su impacto sobre el régimen jurídico de los empleados públicos. *Revista Vasca de Gestión de Personas y Organizaciones Públicas* (15), 82-99.
- Denhardt, R. B. (1993). *Theories of public organization*. Wadsworth Publishing.
- El proyecto Sedipualb@ www.sedipualba.es
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ministerio de Asuntos Económicos y Transformación Digital. Estrategia Digital de España 2025.
- Plan de Digitalización de las Administraciones Públicas 2021-2025.

¹⁵ Agencia Oberta de Catalunya.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Reglamento sobre la Europa Interoperable (Interoperability Act Europe).

Reglamento Europeo sobre Inteligencia Artificial.

Wadhvani Foundation. (2024). Los obstáculos para la transformación digital de la administración pública: Una inmersión profunda en los principales retos.

Wolters Kluwer. (2024). 6 consejos para superar la resistencia al cambio en la transformación digital.